July 1, 1996

Military Operations Research Society

Simulation Data and its Management Mini-Symposium (SIMDATAM '95)

Charles E. Gettig, Jr, Chair

Proceedings Edited By: Dr. Julian I. Palmore
University of Illinois

28-29 March 1995
Center for Strategic Leadership
United States Army War College
Carlisle, Pennsylvania

101 South Whiting Street •Suite 202 • Alexandria, VA 22304 • (703) 751-7290• Fax: (703) 751-8171
E-mail: morsoffice@aol.com

DISCLAIMER

The Military Operations Research Society summarizes the findings of a mini-symposium conducted over two days by experts, users, and participants interested in Simulation Data and its Management. It is not intended to be a comprehensive treatise on the subject. It reflects the major concerns, insights, thoughts, and directions of the participants at the time of the minisymposium.

CAVEATS

The Military Operations Research Society does not make nor advocate official policy.

Matters discussed or statements made during the mini-symposium were the sole responsibility of the participants involved.

The Society retains all rights regarding final decisions on the content of this Mini-Symposium Report.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	1 July 1996	Simulation Data and its Management Mini-Symposium (SIMDATAM '95) 28-29 March 1995

4. TITLE AND SUBTITLE

Simulation Data and its Management Mini-Symposium (SIMDATAM '95)

5. FUNDING NUMBERS

O & MN

6. AUTHOR(S)

Charles E. Gettig Jr., Chair, Dr. Julian I. Palmore, Proceedings Editor

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Military Operations Research Society, Inc.
101 S. Whiting Street, Suite 202
Alexandria, VA 22304-3483

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office Chief of Naval Operations, N81
Washington, DC 20350-2000

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unlimited; Approved for Public Release

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

These proceedings record the results of a mini-symposium held on 28-29 March 1995. Six Working Groups convened to examine the procedures and technology advances in developing and utilizing simulation data and data management and make recommendations.

14. SUBJECT TERMS

15. NUMBER OF PAGES
I - x + 78 pages

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Sta. 239-18
298-102

CLASSIFIED BY:

DECLASSIFIED ON:

July 1, 1996

Military Operations Research Society

Simulation Data and its Management Mini-Symposium (SIMDATAM '95)

Charles E. Gettig, Jr, Chair

Proceedings Edited By: Dr. Julian I. Palmore
University of Illinois

28-29 March 1995
Center for Strategic Leadership
United States Army War College
Carlisle, Pennsylvania

101 South Whiting Street •Suite 202 • Alexandria, VA 22304 • (703) 751-7290• Fax: (703) 751-8171
E-mail: morsoffice@aol.com

The Military Operations Research Society

The purpose of the Military Operations Research Society (MORS) is to enhance the quality and effectiveness of classified and unclassified military operations research. To accomplish this purpose, the Society provides media for professional exchange and peer criticism among students, theoreticians, practitioners, and users of military operations research. These media consist primarily of the traditional annual MORS symposia (classified), their published proceedings, special mini-symposia, workshops, colloquia and special purpose monographs. The forum provided by these media is directed to display the state of the art, to encourage consistent professional quality, to stimulate communication and interaction between practitioners and users, and to foster the interest and development of students of operations research. In performing its function, the Military Operations Research Society does not make or advocate official policy nor does it attempt to influence the formulation of policy. Matters discussed or statements made during the course of its symposia or printed in its publications represent the positions of the individual participants and authors and not of the Society.

The Military Operations Research Society is operated by a Board of Directors consisting of 30 members, 28 of whom are elected by vote of the Board to serve a term of four years. The persons nominated for this election are normally individuals who have attained recognition and prominence in the field of military operations research and who have demonstrated an active interest in its programs and activities. The remaining two members of the Board of Directors are the Past President who serves by right and the Executive Vice President who serves as a consequence of his position. A limited number of Advisory Directors are appointed from time to time, usually for a one-year term, to perform some particular function. Since a major portion of the Society's affairs is connected with classified services to military sponsors, the Society does not have a general membership in the sense of other professional societies. The members of MORS are the Directors, persons who have attended a MORS meeting within the past three years and Fellows of the Society (FS) who, in recognition of their unique contributions to the Society, are elected by the Board of Directors for life.

MORS is sponsored by:

- The Deputy Under Secretary of the Army (Operations Research)
- The Director, Assessment Division, Office of the Chief of Naval Operations
- The Director of Modeling, Simulation and Analysis, Deputy Chief of Staff, Plans and Operations, Headquarters, US Air Force
- The Commanding General, Marine Corps Combat Development Command
- The Director of Force Structure, Resource and Assessment, The Joint Staff
- The Director Program Analysis and Evaluation, Office Secretary of Defense

PREFACE

Simulation Data Management is a thorny topic. Everyone in the Military Operations Research community knows that models and simulations contain data and databases. The essential role of data in any modeling of real world systems is described by many authors. There may be a mathematical description of the interactions between parts of a model but the initialization and scaling of the interactions must be given by data and data bases. Why is this so? The reason is that real world systems are being described and real world systems have shapes, sizes, and other physical attributes that require measurements to define.

These Proceedings of the Mini-Symposium on Simulation Data and its Management (SIMDATAM '95) begin with an Executive Summary. The Executive Summary contains discussions and conclusions from every working group. Following the Executive Summary, in Chapters 2-6, are the final reports of the five working groups on Verification, Validation, and Certification, Standardization, Emerging Technologies, Data Security, and Research. The Synthesis Group report is in Chapter 7.

CAPT Lee Dick, in his address to SIMDATAM '95, discussed the problems and concerns of simulation data management. His revised address appeared in the December 1995 issue of *PHALANX*. In turn, his *PHALANX* article appears in these Proceedings as Appendix C.

In editing these Proceedings I faced the problem of "bullets" and "phrases" substituting for sentences. I hope you, the reader, will find my solution to this problem acceptable.

Julian Palmore
Editor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The workshop on Simulation Data and its Management was sponsored by the Military Operations Research Society (MORS) and conducted at the Center for Strategic Leadership, United States Army War College (USAWC) on 28-29 March 1995. It was attended by 78 military and civilian analysts. Most of the workshop was devoted to individual working group sessions. The agenda is in Appendix A. Detailed working group discussions are included in the working group final reports. These are: Chapter 2, Verification, Validation and Certification; Chapter 3, Data Standards; Chapter 4, Enabling Technologies; Chapter 5, Security; Chapter 6, Research; and Chapter 7, Synthesis Group.

Numerous issues were raised in each working group. These are reviewed in detail in the following chapters. To provide a general reference to the overall issues and recommendations, some points from each working group are included in this chapter. See each individual chapter for the complete set of issues and recommendations by subject area.

1. Verification, Validation, and Certification (VV&C)

Issue: How should the problem of Service "blessed" data be addressed? The M&S profession should move away from service specific standards toward universal standards. User VV&C should depend on substantive issues and conditions. However, political questions are involved. How do we proceed to move toward these ideals?

We propose three choices. (1) Declare that the concept doesn't exist any more. User VV&C must be sufficient and any claims of study validity must be based on the merits of the VV&C procedure. (2) Declare that VV&C is irrelevant in cases involving interservice problems. (3) Declare in interservice cases that user data VV&C be placed under Joint or PA&E control.

Discussion

Data verification, validation and certification (VV&C) is naturally segmented into data producer VV&C and data user VV&C. The proper measure of verification and validation (V&V) is a set of caveats on the results, rather than an attempt to describe the V&V in terms of levels.

In all cases, the overall result of data use depends not only on the process but also on the quality of analyst/user. No process can substitute for the active and interested effort by competent people. A mindless application of rules, whether simple checks of formats or complex data transformation algorithms, is insufficient to produce good quality results. Standard databases of producer VV&C data do not justify their mindless use in Modeling and Simulation (M&S) for analysis. This implies that user VV&C is required.

Certain tests, based on data type, should be required in each V&V process prior to certification. Metadata, data about the data, are subject to the VV&C process. Experts in the various data types will be needed to define the particulars. However, the existence of minimum standards should not be used as

an excuse for not doing better. Producers and users should examine the costs and benefits of going beyond the minimum standards on a case by case basis.

Just as configuration management of models is required to implement VV&A, configuration management is required for VV&C. Both the producers and the users of data must implement data configuration management. It needs to be added to the model configuration management by the user and is an organizational responsibility of the data producer.

There remain several unanswered questions.Who pays for VV&C? How much VV&C can be afforded? How should the problem of Service "blessed" data be addressed? How do we proceed to move toward these ideals?

Clearly a vigorous program of VV&C will not be cost free. The segregation of VV&C into producer and user segments allots the direct responsibility for the costs to the appropriate parties; however, the funds may remain to be found. The M&S profession should move away from service specific standards toward universal standards. User VV&C should depend on substantive issues and conditions. However, political questions are involved. Good producer VV&C will lead to better studies and reduced demands on users to search for errors in the data. The savings that result from good producer VV&C must be partially invested in user VV&C. As a practical matter, VV&C is impacted by the number of models, number of formats, lack of standards, etc., which complicate the data problem. As a result, improvement in data VV&C will not be immediate.

2. Data Standards

Issue: The primary issue that concerns the data standardization process is the willingness of organizations to expend sufficient resources. The resources of money, personnel and time needed to make a legacy system conform to a data standard are huge.

To meet the interoperability objectives of the future, organizations must aggressively standardize their data and data systems. The group suggests that DoD categorize and focus its efforts to standardize. It is important to encourage organizations to willingly standardize the data that they share with others.

Discussion

Everywhere one turns these days there is talk of "Information Highways" to share information between systems or an "Infosphere" where one can get the information needed anywhere at any time. It is important to link systems and exchange data via standard data items. Data standardization provides the foundation for linking systems and organizations that are separated geographically and organizationally.

Standards are built by a consensus of all of those involved. The standards should start with the data producer. And agreement should be built with the customer and other subject matter experts. Standards established cooperatively are more easily accepted and are more enduring.

3. Emerging Technologies

Issue: The primary issue revolved around how the enabling technologies in computer science could be implemented in an organ-

izational and political structure that may or may not change itself in order to accommodate the potential value added by those technologies.

4. Data Security

This group recommends that a strong emphasis be given to distributed data storage, distributed processing and a wide dissemination of analysis results back into the 'community' into which the data capacity and processing capability is found.

Discussion

The group met to discuss enabling technologies in computer science for models and simulations. The areas of technology addressed were increased data flow, increased computer speed, and increased data storage.

Secondary issues were the value of distributed or centralized data base controls, the use of commercial software to perform 'business tasks' in the military analysis community, and the value of a DoD level Data Technologies working group to access the usefulness of new computer science technologies as they emerge from the 'civilian' and 'military' research communities.

This group recommended that commercial off the shelf (COTS) be used wherever possible for the management of data, and that the software of weapons themselves would continue to be 'developed' packages. We did not recommended that a DoD level Data Technologies group be established. We did recommend that MORS establish a working group on Cultural Changes.

Discussion

Issue: How would we even know if our data or systems were compromised? Often, data is undervalued until it is lost. And, if DoD is to rely on M&S for operational needs, we must have means to guard against disruption of capabilities in time of national emergency.

The Defense Goal Security Architecture (DGSA) should be tried on a current DoD M&S system. Not only would this pilot program provide a real world test of the DGSA framework, but it would establish a programmatic prototype for addressing real world M&S security needs.

Discussion

Modeling and simulation (M&S) data must be protected whether it is in storage, in transit, or being processed. Since data in DoD models and simulations will be found in all of these states, the rest of this paper addresses security of the entire M&S system, rather than just the data in storage.

A full range of security services is required including protection of data from unauthorized disclosure or modification, protection of users from unauthenticated participants or denial of authenticated participation, and protection of systems from penetration or sabotage.

Protection of information must address not only issues of national security and the protection of key defense capabilities, but additionally must address the protection of proprietary data and intellectual property.

While achieving the desired levels of pro-

tection, we must implement modeling and simulation (M&S) capabilities that cross the spectrum of DoD functionality, i.e., Advanced Concepts and Requirements (ACR), Research, Development and Acquisition (RDA), and Training, Exercises, and Military Operations (TEMO).

To accomplish these many purposes, DoD requires simulations wherein participants operating at various levels of classification can interoperate on a battlefield composed of live, virtual and constructive components.

To achieve both the desired level of protection and the full operational capability needed will not be easy. Although many security measures may be implemented and working fine, it takes only one exploitable weakness to compromise the security of the entire system. As computers are interconnected, targets for exploitation become more lucrative; and it becomes more likely that the single weakness needed for access can be found. Protection is never going to be completely assured. Thus, risk management, not risk avoidance, must be incorporated into the M&S protection philosophy.

Engineering and operational tradeoffs will be required. The Defense Goal Security Architecture shows promise as a framework in which the vision of fully functional secure M&S can be achieved. Within this framework, research is moving forward, fundamental concepts are being developed, and a methodology to engineer secure systems is being pursued. There will be no "magic bullet" which solves all of the requirements. Rather, a layered approach to implementing security services will be needed.

Safeguarding the integrity of all data against internal and external threats is a key issue. Would we even know if our data or systems were compromised? Often, data is undervalued until it is lost. And, if DoD is to rely on M&S for operational needs, we must have means to guard against disruption of capabilities in time of national emergency.

The aggregation of data may result in the need to protect the data at levels above that of the disaggregated pieces. It is not clear how to know when the threshold for added protection is crossed, nor is it clear who actually and authoritatively makes that determination and on what grounds.

Secure interoperability would ideally mean components at various levels of security could communicate and use another's data without compromise. Presently, simulations are operated at the highest level of classification of any of the components. It might be possible to have some simulation components at a high level of security classification that can effectively hide the classified data and processing from other simulation components who are operating at a lower security level. Procedures to enable this multi-level mode of operation need to be developed. A critical issue in developing procedures will be to address when inferences can be drawn as to the classified data and when capabilities can be inferred from an accumulation of the released sanitized data.

A forum must be established where M&S security requirements can be delineated. While we have made a few overarching statements of requirements at this working group, a detailed set of requirements must be forthcoming in order that they can be ad-

dressed. The MORS community should develop intellectual, engineering and automated tools to assist in the identification, development, management, and evaluation of security issues for M&S data.

5. Research

Issue: Key research areas should be standardization, bandwidth, and search and retrieval tools. Research should be conducted on standards for data representation and data transfer, methods for optimizing data transfer, and use of advanced Internet tools for data access and retrieval.

Discussion

While many of the research areas we advocate will be pursued (quite naturally) by the commercial/private sector (we expect the entertainment industry to continue as a leader in this area), the government should consider how it can best finance, direct, or at least influence research in the recommended areas. Issue Areas are Standardization, CPU Performance, Bandwidth, Integration and Interoperability, Aggregation, Search and Retrieval Tools.

The Research Working Group recommends that the Government sponsor or promote research in the following several areas: Methods for optimizing data transfer: standards for data representation and data transfer; standards for performing and documenting VV&A/C; approaches for optimizing VV&A/C; standards for nomenclatures, terminologies, and dictionaries; techniques for consolidating nomenclatures and merging taxonomies; opportunities for precalculating, pre-storing, and then replaying complex physics-based scenarios; compression algorithms; intelligent agents as surrogates for data transfer; distributed data systems; distributed processing; semantic translation; methods for reconciling differences in units of measure, resolution, and fidelity; experiments to give analysts insight into how one could and should aggregate data; use of advanced Internet tools for data access and retrieval; construction of intelligent search and retrieval tools; creation of tools for identifying and retrieving mathematical equations and algorithms; techniques for optimizing data representation and data storage; investigations into the "appropriate" use of OO; relational, and textual databases.

6. Synthesis Group

Issue: There is accelerating growth of data, databases, computers, transmission rates, and storage capacity problems. Commendable progress in solving yesterday's problems has been made, but there is an onrush of new problems yet to be solved.

MORS should execute a program to act on the appropriate recommendations from this workshop. This will enable us to come to grips with the fact that we are caught up in¥ —and interact with—an exhilarating dynamicqueue of unknown parameters and questionable stability in simulation datamanagement.

CHAPTER 1

INTRODUCTION

Charles E. Gettig, Jr., Chair and Colonel Stephen D. Williams, USA, Co-Chair

1. SIMDATAM Background

In 1991 the Deputy Secretary of Defense instituted an initiative to strengthen the application of modeling and simulation (M&S) in the DoD community. This increased emphasis has stirred efforts to improve policy, procedures, and techniques in developing inter-operability standards and protocols among DoD M&S activities. This led to the development of the SIMDATAM series. In an inter-operability environment, it focuses on simulation data development, standardization, verification and validation, security, emerging technologies, research, transformation, storage, maintenance, and transmission.

The first symposium SIMDATAM 93 was held 16-18 November 1993 at Falls Church, VA. It concluded that new data base and other technologies have great potential and the emergence of numerous complex, high tech models and simulations has led to specialization.

The SIMDATAM 95 workshop is a follow on to the symposium. The planning started in June 1994 at the 62nd MORS Symposium. The result of the planning and the Senior Advisory Group (SAG) guidance is in the Terms of Reference (TOR), which is attached in Appendix B.

The goals and objectives differed only in the focus of the effort. SIMDATAM 95 was conducted as a workshop rather than a symposium.

The co-proponents for SIMDATAM 95 are: The Director for Force Structure, Resource and Assessment, The Joint Staff; The Deputy Under Secretary of the Army (Operations Research); Director of Modeling, Simulation and Analysis, Deputy Chief of Staff, Plans and Operations, HQ USAF; The Director, Assessment Division, Office Chief of Naval Operations, and the Commanding General, Marine Corps Combat Development Command.

2. Workshop Objectives

The goal of this workshop was to examine processes and technology advances in developing and utilizing simulation data and data management and make recommendations.

The objective of SIMDATAM 95 was to determine, examine, formulate, and recommend, military operations research standards, procedures, and technology, applicable to simulation data and its management. This workshop made recommendations regarding SIMDATAM standards and procedures and examined and recommended advanced technologies in data management.

Within the framework of goals and objectives, the appropriate working groups were tasked to answer the following questions.

(1) What is the role of verification, validation and certification in databases and is there feasibility and utility in the establishment of a DoD level standing VV&C Group? (2) How can data and data systems be standardized? Is there feasibility and utility in the establishment of a DoD standing Standards Group? (3) What current and emerging technologies would enable the collection, storage, retrieval, and dissemination of simulation data? (4) What are the solutions to the data security classification issues? (5) What is the pertinent current research on simulation data and its management? How can it be expedited and applied to current models and simulations?

3. Conduct of the Workshop

The workshop achieved the above goals and objectives over a 2 day time frame. The four hour plenary session was devoted to guest speakers and a tutorial. The remainder of the session was devoted to working group sessions, except for a short plenary review session at the end of the second day. The reporting phase of the workshop will be accomplished by follow on sponsor reports, formal publication of the proceedings, and articles in the professional media.

The opening plenary session featured the following speakers.

Keynote speaker was Captain Lee Dick, Director, Modeling, Simulations & Analysis, Space & Naval Warfare Systems Command, Arlington, VA. He spoke on "Simulation Data And The Need for Standardization."

Primary speaker was Col James E. Shiflett, Project Manager, Combined Arms Tactical Trainer, STRICOM, Orlando, FL. He spoke on "Setting Data Standards."

Tutorial speaker was Mr. Roy Scrudder, Computer Scientist, Systems Engineering Division, Computer Sciences Corp, Ft. Huachuca, AZ. His topic was "Data Modeling."

Working groups met in the afternoon of the first day and all of the second day.

WG1: Verification, Validation and Certification (VV&C) in Databases
Chair: Dr. Dean S. Hartley III, Martin Marietta Energy Systems, Oak Ridge, TN
Co-chair: Mr. Howard G. Whitley III, USACAA, Bethesda, MD
Key focus: The role of verification, validation and certification in databases and the feasibility and utility in establishing a DoD level standing VV&C Group.

WG2: Standardization of data and data systems
Chair: Major Walter L. Swindell II, USA, TRAC Ft. Leavenworth, KS
Co-chair: Major Karen S. Barland, USAFSAA, Washington DC
Key focus: Standardization of data and data systems and the feasibility and utility on establishing a DoD Standards Group. Focus on the data requirements and data management implications of achieving Dominant Battlefield Awareness (DBA) in 2002.

WG3: Enabling Technologies
Chair: Mr. Steve T. Boyd, USAFSAA, Washington DC
Key focus: The enabling technologies that would be useful to the collection, storage, retrieval, and dissemination of simulation data and the contribution of these to Domi-

nant Battlefield Awareness in 2002.

WG4: Data Security
Chair: Ms. Janet Morrow, U. S. Army NGIC. Charlottesville, VA
Co-chair: Ms. Lana E. McGlynn, US Army MSMO, Arlington, VA
Key focus: The solutions to the data security and classification issues.

WG5: Research
Chair: Dr. William A. Carpenter, The MITRE Corporation, McLean, VA
Co-chair: Mr. Wesley L. Hamm, The MITRE Corporation, McLean, VA
Key focus: The pertinent current research on simulation data and its management? Identify the research that will contribute to Dominant Battlefield Awareness in 2002.

WG6: Synthesis Group
Chair: Mr. Clayton J. Thomas, FS, HQUSAF/SAN, Washington, DC
Co-chair: Mr. Eugene P. Visco, FS, Office of the DUSA (OR) Washington, DC
Technical assistant: Major Kevin Giles, USAWC, Group Systems V Software
Key focus: This group reviewed and synthesized the working deliberations. It reported on findings, identified over arching issues, and prepared recommendations.

CHAPTER 2

VERIFICATION, VALIDATION AND CERTIFICATION

Dr. Dean Hartley, Chair, and Mr. Howard Whitley, Co-Chair

1. Working Group Objectives

Key Focus: What is the role of verification, validation and certification in databases?

We examined the following questions.

What is data VV&C?
What are the quality issues?
What are the certification issues?
Can the VV&C of input data be divorced from the source of the methodologies?
What are the issues involving certification and accreditation? What is the difference between the two?
How does one ensure the quality of the input data?
What techniques are being used to do this?
What are the techniques for VV&C of input data and its associated interaction with methodologies?
What software capabilities and graphics are being used to ensure the data correctly represents the phenomena intended?
How can VV&C be expedited and applied to current models and simulations?

We discussed and made recommend actions on the development of a data source catalog, which would document data origins, lineage, and include subject matter experts.

2. Conduct of the Working Group

Agenda
Opening Statement - Hartley
Self Introductions - WG 1 Members
WG Questions - WG 1 Members

Successful tests and experiences with lessons learned are encouraged to be shared between all.
SIMDATAM Questions- Hartley/Members

Presentation- Hartley

Speakers: None.

3. Presentations: None.

4. Discussion

The working group was conducted under the assumption that the members represented sufficient breadth and depth in the simulation data field that their experience and opinions would provide a firm basis for decisions. This assumption was borne out by the results of the working group. Because of this assumption, both agreement and disagreement on issues were regarded as significant. This section will cover the preliminary and intermediate areas of the working group; areas of disagreement or areas that needed resolution in some other forum are discussed in the Issues section; and areas of agreement in which action is needed (or should be avoided) are discussed in the Recommendations section.

Rationale for Action

The first order of business was to develop a

rationale for VV&C, considering that a serious program would add visible costs. The following reasons discussed for performing VV&C included both defensive positions and more proactive positions.

- "are lazy - don't do good checking now"
- want credibility
- want external check
- want authority behind data
- pin blame/avoid blame
- want documented sources
- complexity of M&S (especially Distributed Interactive Simulation) requires that data at elementary level be "good"
- want support for presentation of results
- proactive - VV&C will improve results
- have a desire to know what we are doing, VV&C will help
- what we are doing with data is important, VV&C can be critical
- information on data precision is a metric for simulation results
- VV&C provides standards for measuring quality of data
- VV&C provides sufficient information to permit proper use
- VV&C permits less work by analyst using model, increases efficiency
- data are part of model, so VV&C is part of VV&A
- VV&C coincides with software maturity model precepts
- data providers have responsibility to users to provide VV&C
- VV&C supports reuse of data

The conclusion was that there are sufficient reasons for VV&C.

What Are Data?

The next question was an elucidation of our concept of the meaning of data. This provided a guard against simplistic solutions based on a naive concept of data consisting solely of numerical descriptions of physically measurable quantities. Data include:

- complex - contains algorithms, etc.
- numerical measurements of physical characteristics
- assumptions
- equipment performance and vulnerability measures
- environmental
- scenarios
- metadata/standards
- cognitive
- test results
- model derived data
- classification
- doctrine
- unit performance data
- future systems
- human factors
- political data
- financial data
- made up data
- verbal statements

We also discussed the problem that some data are so complex that they are best expressed as a model rather than as a multidimensional table of numbers. An example was the combat effectiveness of a military unit, which depends on so many factors in such complex ways that a complete table of numbers would be unmanageable and any request for a single number could be misunderstood. Such situations would lend themselves better to collaborative analysis than to databases.

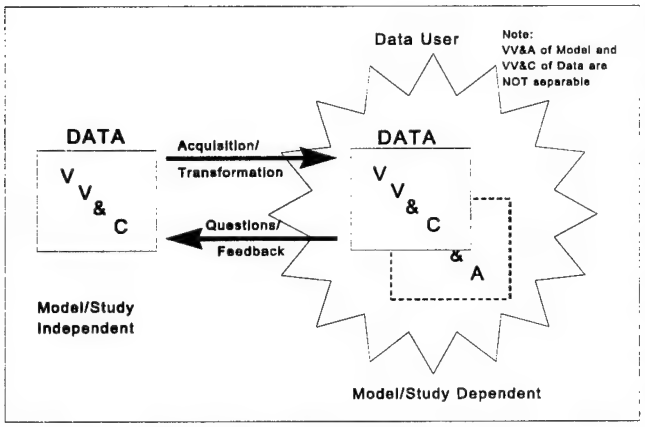

Figure 2-1. Simple VV&C Process

Data also have important attributes, such as provenance (heritage or pedigree), degree of perishability, classification, descriptions, type (field test, bench test, or modeling results), and VV&C test results. These attributes are metadata. They permit the proper understanding and use of the data. For example, "5" is recognizable as a number; however, more information is required to decide whether this datum represents a number of tanks, divisions, rate of fire, or some other useful item of information. Metadata are also data.

VV&C Definitions and Process

The working group considered what should be meant by verification, validation and certification. After discussion several central concepts were agreed on. The central differentiation was represented by: validity is a statement that '5.6' is the right number, whereas verification states that '5.6' is the number that was supposed to be entered. There was a concern that excessive rigidity would lead to the belief that tests make validity, not truth. Examples were discussed showing that validity depends upon particular situations, e.g. where the relative values of a set of numbers might be more an indication of validity than the actual values. Thus the validity of a number can be relative to the values of other numbers. The classification context can change what the valid values are. In general, the criteria for validity should be requirements driven. The assumptions and context define validity and the statement of validity should be that the data are valid means that these are the best data within the given context/assumptions (which must be explicitly stated). As a corollary, complete and accurate definition of a variable is required for its valid use. Verification and validation are processes for improving quality and reducing the risk of being wrong.

At this point the Defense Modeling and Simulation Organization (DMSO) definitions (from DoD 5000.59, DoD M&S Master Plan) were introduced and compared to the working group concepts. The difference between producer VV&C and user VV&C in the DMSO definitions had been a critical working group concept and was accepted as a requirement. The wording of the definitions caused some concern until the working group decided that the addition of a definition of "data" as used in the VV&C definitions could solve the problem. "Subject Data" is used to refer to the data content that is desired for use in a model or simulation.

In addition to the definitions, the working group constructed a process description of VV&C. The application of simple definitions for VV&C promotes quality by inspection. Quality by inspection can reduce errors; however, it is insufficient for a total quality approach. Quality by process design, or engineered quality produces more profound effects.

The simplest process explanation is shown in Figure 2-1, where a single data producer and a single data user are postulated. The producer gathers, creates, receives, or in some fashion acquires his data. In general, his mode of operation is model/study independent. The producer verifies, validates and certifies his data. The user, generally driven by a particular model/study need, acquires and (possibly) transforms the data. The user verifies and validates the data for use in the model, perhaps asking questions of the producer or giving feedback on problems identified in the data. Once the user is satisfied, he certifies the data. Notice, however, in the figure that the data VV&C is shown to overlap the model VV&A process. This is done because the VV&A of models and the VV&C of their data is not independent.

The discussion brought out the fact that there is a substantial data pull process that originates the data, as opposed to a data push, in which the producer creates data completely independent of user needs. In the data pull process, the process is initiated by a request for new data by the user.

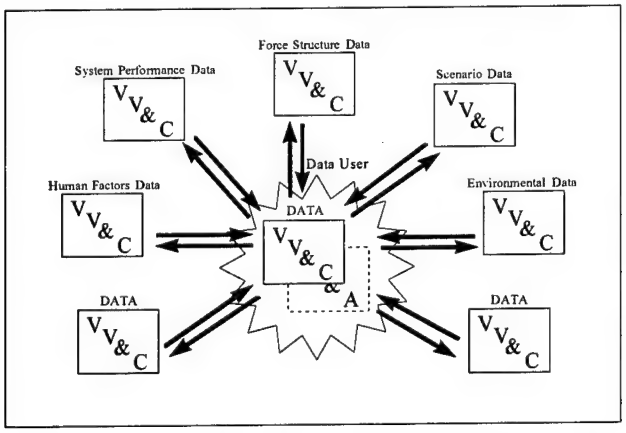

Figure 2-2. More Realistic VV&C Process

Figure 2-2 expands the situation shown in Figure 2-1 to the current situation for a user. Each user has not one, but in general has several to very many data producers to deal with. This complicates the problem of performing user VV&C. Figure 2 could be further expanded to show that the general data producer supplies not one but many users. The impact of this is that tailoring the data for a single user adds a burden to the producer, whereas providing a generic product that fits the needs of at most one user adds to the burden of the user VV&C process.

In all cases, the overall result depends not only on the process, but also on the quality of analyst/user. No process can substitute for the active and interested application of effort by competent people. A mindless application of rules, whether simple checks of formats or complex data transformation algorithms, is insufficient to produce good quality results. The savings that result from good producer VV&C must be partially invested in user VV&C.

Techniques and Tools

The need for data VV&C was emphatically substantiated by the description of the errors found in Defense Intelligence Agency (DIA) supplied data. Some of the errors were described as formatting errors and some as substantive errors.

Considerations

There are many different types of techniques and tools that can be used for V&V. Some may be useful for verification, some for validation, and some for both. The applicability and functionality of each depends on the type of data. Often the tools are hardware or operating system dependent and dependent on the type of storage, including particular data-

base management software. None of the tools or techniques is universal in applicability.

Tests

Several tests and tools were discussed and are listed below.

- range tests by variable
- tests for blanks
- tests for repetitions, single and in blocks
- compatibility checks/loader checks
- statistical tests (testing for too good or too poor a fit to a distribution representing data)
- calibrate - current data to a standard (e.g. time based data) in a model-test-model analog
- historical benchmarking
- compare against other data, other sources (after the fact), or asking dual sources for data
- keep newest data
- name checks (e.g., M1A1 vs. M1-A1)
- old version vs. new version with flags on excessive differences ("different" are not necessarily "wrong")
- panel of experts
- results oriented - where data comes from may engender trust; number of times used by others may engender trust
- graphic presentation for anomalies
- algorithms for anomalies
- suites of tests such as developed at USCENTCOM

Certain tests, based on data type, should be required in each V&V process prior to certification. Experts in the various data types will be needed to define the particulars. However, the existence of these minimum standards should not be used as an excuse for not exceeding the minimum. Producers and users should examine the costs and benefits of going beyond the standards on a case by case basis.

Configuration Management

Just as configuration management of models is required to implement VV&A, configuration management is required for VV&C. Both the producers and the users of data must implement data configuration management. Configuration management includes database administrator, access control, record keeping, and retrieval functions. In particular, data configuration management needs to be added to the model configuration management by the user and is an organizational responsibility of data producer.

Responsibilities

Both producers of data and users of data bear responsibilities with respect to VV&C of data.

The producer is responsible for:

- performing producer VV&C
- producing and maintaining metadata
- performing data configuration management
- initial communication of data and metadata
- subsequent communication of any errors found or other changes

The user is responsible for:

- communicating with the producer to understand the data
- performing user VV&C
- giving the producer feedback on any data problems or errors found

- performing data configuration management
- doing good work

Generalities

VV&C does not reduce the responsibility for good work, it merely makes it more possible to bear.

As a practical matter, VV&C is impacted by the number of models, number of formats, lack of standards, etc., which complicate the data problem. As a result, improvement in data VV&C will not be immediate; however, that is no excuse for not starting.

5. Issues

There are several issues that the working group raised, but was not competent to solve.

Who pays for VV&C? Clearly a vigorous program of VV&C will not be cost free. How much VV&C can be afforded? The segregation of VV&C into producer and user segments allots the direct responsibility for the costs to the appropriate parties; however, the funds may remain to be found.

What should be done about different procedures by different organizations? In some cases there are close ties between producing organizations and using organizations, wherein data needs are closely matched by data production. In other organizations, this is not the case. These difference will become acute if a central repository is created. Even if no new organizations are created, the increasingly joint nature of modeling and simulation will create new demands for cross-service data flows that have not previously existed.

What should be done about differences in the way users and producers look at validity? In a perfect world models and simulations would not require data that are unavailable and producers would not create data in forms of little use. However, both situations currently exist and must be accommodated.

Does VV&C require data variances as part of the metadata or is this just a "nice" thing? A proper understanding of the data requires an understanding of the level of precision, which includes information about the variance and modal nature of the data. This information is often lacking and not all users understand the need.

A central data "scrub shop" has been proposed. Such a facility could facilitate data acquisition by users. It would take raw data, test it, clean up errors, and add comments and recommendations for usage. However, there are questions about the competence that such a facility would require and the duplication of expertise to support such competence. There is also the question of centralization vs. decentralization.

With regard to any central data reference database, there are several issues, three items are required to make user VV&C possible:

- Sources
- Metadata
- V&V tests performed (quality profile)

Other items might include:

- Reasonably complete data, a la Army Force
- Planning Data and Assumptions documents (AFPDA)
- Subject matter experts
- Example data

- History of use
- Should such a database be universal (all services, all types of data) or non-universal?
- Such a database must have visibility of source for variations of quality, reliability, production methodology, etc., among sources.
- It should not be too easy to get incompatible data from the database.
- The organization of the database (retrieval strategy or strategies) is important.
- All of the time saved in gathering data is not available as a time savings, some must be applied to user VV&C.
- Would such an organization create a requirement for an intermediate kind of certification, between producer and user?
- If data pull predominates over data push, how much of the available data are actually usable by any other user than the one who requested it? Such a situation might seriously limit the value of a central database.

How should the problem of Service "blessed" data be addressed? Three solutions were proposed, with no agreement on any one.

- Declare that the concept doesn't exist any more. User VV&C must be sufficient and any claims of study validity be based on the merits of the VV&C procedure.
- Declare that VV&C is irrelevant in cases involving interservice problems.
- Declare that user data VV&C in interservice cases be placed under Joint or OSD (PA&E) control.

How should access to certified data be handled? Is it open to all based on reasonable clearance and need-to-know restrictions or are some data to be restricted to "internal" users only? Are there classes of data that can be released to one set of users and not to another, aside from an internal vs. external classification? Because of data differences, a variety of procedures and standards are required. A working group of experts is required to define the minimum standards for each type of data.

Producer responsibility does not end with transfer of data. What are their responsibilities? For example, when data sources are always obvious, nor is the data background or the subject matter experts who produced the data?

The issue of aggregated data VV&C as opposed to "atomistic" data VV&C is not clear. When a producer creates such data, what information should be passed to the users, what procedures should be used to create the data, and what VV&A procedures should apply?

6. Recommendations

There are three general recommendations. (1) Certain tests should be required (depending on data type) for all data. (2) Metadata is required and needs to be subject to VV&C. (3) The appropriate measure for the quality of V&V consists of caveats rather than any notion of levels of V&V.

There are two recommendations with respect to producer VV&C. (1) Configuration management is a required responsibility for VV&C producers and should include user lists and an update notification process. (2) Care should be taken in the use of word "certified." Unchanged producer data that have been certified retain that certification. Certain changes, such as excursions may retain the producer certification for the bulk of

the data as long as the modifications for the excursions are plainly identified. The excursion data must be user certified. Similarly, corrections to the data must be user certified and identified, with the bulk of the data retaining producer certification; however, the user has the responsibility to give feedback on problems to the producer.

There are five recommendations with respect to user VV&C. (1) Data/modeling interactions require "managed collaborative analysis" for resolution. These cases occur when the required data are complex and depend on the use to which the data will be put. (2) Transformation procedures of producer data to model input data requires VV&C of the procedures. (3) Standard databases of producer VV&C data do not justify mindless use in M&S for analysis. This implies that user VV&C is required. (4) An analyst guide for models (new and old) is useful forVV&C. In many cases it should be required. (5) The M&S profession should move away from service specific standards toward universal standards. User VV&C should depend on substantive issues and conditions.

CHAPTER 3

STANDARDIZATION

Major Walter L. Swindell, II, USA Chair and Major Karen Barland, USAF, Co-Chair

1. Working Group Objectives

Key Focus: How can data and data systems be standardized? What are the requirements and data management implications to achieving Dominant Battlefield Awareness (DBA) in 2002?

Examine:

(1) Current and emerging standards for service data sharing:
- Standards for terrain database content and transfer format
- Architecture to interconnect simulations/simulators

(2) What are the issues associated with:
- Protecting legacy data
- Standardization of data format
- Data input and output
- SQL

(3) How do we reconcile data standards with major programs?

(4) What is the Corporate Information Management (CIM) Plan?

2. Conduct of the Working Group

Agenda
28 March 95
Introduction and Welcome (MAJ Walter Swindell)
Recommendations from SIMDATAM '93 (MAJ Walter Swindell)
"DIS Need for DoD Data Standards" and the Data Standards and Repositories Special Interest Group (MAJ Walter Swindell)
The Model & Simulation Resource Repository (MSRR) & the Universal Threat System for Simulations (Roy Scrudder)
Data Verification, Validation & Certification (VV&C) (Susan Solick)
Wrap Up Discussion (All)

29 March 95
Introduction & Recap (MAJ Walter Swindell)
The Conventional Force Data Base & Master Simulations Data System (Mike Hopkins and John Anzevino)
The C2 CORE Model (Robert Walker)
The Close Combat Tactical Trainer (CCTT) (Robert Wright)
Developing Combat Instruction Sets for Computer Generated Forces (Brian McEnany)
Working Group Discussion (All)
The Corporate Information Management (CIM) Strategic Plan (John Graves)
Working Group Discussion (All)
Prepare Group Summary Presentation (MAJ Walter Swindell and Maj Karen Barland)

3. Presentations

Summary and Excerpts of Recommendations from SIMDATAM '93:

MAJ Swindell presented a summary of SIMDATAM '93. He briefed some of the work that has been done to respond to rec-

ommendations from the previous SIMDATAM. Two of the recommendations were to form VV&C and Data Standards working groups. Through DMSO these groups have been established. The VV&C working group is working to establish policies and guidelines for doing data VV&C and to establish a directory of authoritative data sources. The Data Standards working group is working to promulgate DoD standards, to include the DIS community.

"DIS Need for DoD Data Standards" and the Data Standards and Repositories Special Interest Group.

The Data Standards working group presented a position paper to the DIS Working group to express the need for DoD data standards in the DIS environment. A recommendation was presented to form a DIS Special Interest Group (SIG) to address this issue. The Data Standards and Repositories SIG met in March.

The Model & Simulation Resource Repository (MSRR)

The MSRR is a project sponsored by DMSO and is a distributed repository through the World Wide Web (WWW) which gives easy access to hyper-text service. It provides directories and catalogs of information about models and simulations, databases, meta-data, data models, process models, algorithms, and such. It does not provide data element descriptions. Those are found in the Defense Data Repository (DDR). MSRR provides a valuable service to the M&S community by detailing information and points of contact for models, databases, and other resources.

Data Verification, Validation & Certification (VV&C)

Ms. Solick showed and discussed the DIS Exercise Process Model outlining the relationship between data VV&C and DIS VV&A. She pointed out most of the data V&V should be done first, before the model V&V for DIS exercises, although in the end both V&Vs work together. The group also pointed out that, although not shown on the process model diagram, some analysis or V&V is done after the DIS exercise is over. It is also important to document and record uses of the data and model for future exercises. Mr. McEnany cautioned that some things are done in VV&A as well as VV&C so don't waste resources doing the same process twice. Finally, the entire group realized that the publication of a generic, but firm VV&C template would ease and guide the entire VV&C process as long as the template was not too constraining and allowed for a spectrum of circumstances.

The Conventional Force Data Base (CFDB) and Master Simulations Data System (MSDS)

Mr. Hopkins presented an overview of the CFDB whose purpose is to provide a single source of best-available data for input to a variety of models. The CFDB uses a Data Quality Engineering (DQE) tool to do value-added preprocessing and data accuracy checks on raw data before model input; it greatly reduces scenario preparation time. DQE is based on the data element dictionary and applies business rules to ensure data accuracy to the greatest extent possible and generates error reports on those data items failing to meet standards. Two points of discussion pertaining to data standardization were generated. First, if data standardization is fully accom-

plished, will that eliminate the need for data centers such as the CFDB. Second, will the burden then fall on each model to preprocess and input raw data for model use. The majority of the working group saw other needs for data centers although data standardization would greatly decrease the amount of preprocessing needed before data is input into models. Mr. Anzevino described MSDS interfaces to various models. Both CFDB and MSDS data elements were submitted to the Functional Data Administrator for inclusion in the DDR, but have not yet been approved.

The C2 CORE Model

Mr. Walker presented a briefing on the Command and Control (C2) CORE Data Model. First, he described how data models produce better overall databases, as Mr. Hopkins and Mr. Anzevino discovered when they produced data models of the CFDB/MSDS. Good databases are needed because database to database exchanges are becoming as important as message exchanges. Data models don't limit or dictate how users see data; they do provide a high level specification of inputs and outputs and they do provide a consistent basis for data element standardization. The C2 CORE Data Model provides operational benefits by improving database access and accuracy and by establishing a basis for interoperability. Mr. Walker also cleared up confusion about how the C2 CORE Data Model relates to the DoD Enterprise Data Model; Enterprise Data Model incorporated almost all the C2 CORE Model so if a system is modeled to the C2 CORE Data Model, it's also modeled to the DoD Enterprise Data Model. Mr. Walker also emphasized that DISA does not enforce standards; if the standard (in this case, the C2 CORE Data Model) doesn't work for you, then it is no good and should be replaced. Mr. Walker was asked how low he thought data modeling should be done; he believes we need a very low level of data modeling to do command and control although the resulting standardization may change message formats, etc which will, in turn, impact everything from commanders to the soldier on the battlefield. Issues raised during this presentation include how to decide if the data model is good enough, and should we do reverse engineering data modeling such as the JDBE data modeling or should we start at the top of the data structure and work down.

The Close Combat Tactical Trainer (CCTT)

Dr. Wright gave an overview briefing on the CCTT which is part of the Combined Arms Tactical Trainer. CCTT is a group of interactive workstations which replicates vehicles, weapon systems, and supporting army elements on a simulated real-time electronic battlefield. Data for the CCTT is unclassified and gathered from an amazing variety of sources, both military and non-military. There is V&V done on the data collections which helps identify voids in CCTT so they can be worked around or filled. One important design aspect of CCTT is that all databases are seamlessly linked together so the soldier has access to everything he or she needs. Dr. Wright pointed out how valuable this aspect was since the ease of use and proliferation of systems is necessary to ensure standards are used and survive; Accessibility to the user is the key. Sharing of data between CCTT and CFDB was discussed. CCTT is not code driven and therefore, it is more difficult to share data with code driven systems such as CFDB, although both organizations do gather the same sorts of data and

sometimes from the same sources. The working group also discovered that due to a lack of common data elements, it is rather difficult to share data even in code driven systems. In working on specific training tasks to use in CATT, Mr. McEnany did find a lack of common data elements — for example, only 12 data elements were the same between different logistics databases he was researching.

Developing Combat Instruction Sets (CIS) for Computer Generated Forces

Mr. McEnany presented an overview of the Close Combat Tactical Trainer Semi-Automated Forces (SAF) subsystem. SAF is part of CCTT and provides the supporting environment for manned simulators, including the use of large digitized terrain databases. The problem SAF addresses is how to capture behaviors for training, including system interactions, logistics effects, damage effects, combat instruction sets, and many other aspects of behavior. The Combat Instruction Set provides an end-to-end process for capturing, validating, and implementing tactical behaviors in SAF and is setting the standard for documenting tactical knowledge. One big advantage SAF has is that it has and uses subject matter experts throughout the DoD. These experts guide the SAF developers in making sure behaviors are realistically portrayed. As new behaviors are found, they are documented on CIS forms and scanned into SAF. There is also a Common Activities Table which goes into the requirements document; this table contains activity names which can act as a pointer or key field and allow the user quick and easy access to those subjects he or she is interested in. CCTT has also adopted a standard naming convention for these activity names. Mr. Walker asked if the CIS and outputs had been data modeled and he stated they should be well supported in the C2 CORE Data Model.

The Corporate Information Management (CIM) Strategic Plan

Mr. Graves reviewed the CIM/Enterprise Integration (EI) Strategic Plan. The CIM/EI plan focuses on information effectiveness - the premise that information can be contained in an Infosphere available anywhere, any time, and for any mission. CIM plans to implement that premise by meeting several goals. One of CIM's goals directly related to data standardization is to tie DoD together through the use of quality, shared data and CIM has two objectives in order to meet that goal. The first objective is to derive standard definitions of data, on an aggressive schedule, and use them in shared databases and common information systems. The second objective is to establish delivery throughout DoD of high quality data: including availability, integrity, accuracy, timeliness and security. Mr. Graves said OSD realizes data changes are not free and perhaps the best way to implement changes to legacy systems is to change only mission critical systems on a case-by-case basis in order to keep costs down. OSD's overall desire is to have one owner for each piece of data and to have that piece of data entered into a database once only and shared from that database. OSD is working from the top down, they have completed a strawman "DoD Strategic Plan", and they plan to provide focus and momentum for the implementation of CIM/EI for as long as it takes to implement.

4. Discussion

The need for data standardization is prevalent throughout all of DoD. During this time

of "Information Highways" and "Infospheres", shared information is inherent to global communications. For DoD, this translates into commanders at all levels who are aware of the status of the battlefield through continuous real-time and near real-time situation reports. It means models, simulations, simulators and live service personnel can be connected for combined distributed real-time exercises. Data standardization provides the foundation for linking systems and organizations that are separated geographically and by the color of their uniforms. If all of the data domains were standardized, then writing the interfaces for the connectivity of information systems would be a relatively simple chore.

The working group quickly realized that there are different types of data standards: dictionary standards that deal with describing the data and how the data are formatted (meta-data); standards for the instance data that include the nomenclatures, enumerations, images, and symbols; interconnectivity standards that provide for the communication of systems; and the standards for the sources that provide the data. All of these standards have to be overcome for complete interoperability of models, simulations, and simulators.

There is a lot of work going on in DoD on data standardization. It is imperative that all of these sometimes individual efforts are brought together in a concerted effort. The Office of the Secretary of Defense's Corporate Information Management (CIM) Strategic Plan and the Defense Modeling and Simulation Office's Master Plan have established some near term and long term objectives to facilitate the migration to DoD standards. Policies, programs and guidelines are being erected to ensure that requirements for end-to-end data availability, data integrity and quality, and data security are met.

The group also realized that it is necessary to aggressively pursue areas that need to be standardized. The policy of standardizing on a first come first served basis may not be the answer. Some obscure organizations could come in and select commonly used names for their esoteric entities, thus preventing the common name being used for the common concept. DoD should encourage the functional areas that are used by the masses to step up and standardize first.

5. Issues.

The primary issue that concerns the standardization process is the willingness of organizations to expend the resources. The time, personnel and money involved in making a legacy system conform to a standard is extremely intensive. So, the question then is who should have to pay for the standardization of DoD data?

Other Issues

How long does a standard last? What is the shelf life? Will I have to change again to meet the standard and what is the frequency of change?

Will an organization be forced to be the standard producer of specific data for the community against the producer's will? If an organization is producing data for just a few customers now, will these standards bring in more customers than the organization has the willingness or resources to handle?

Will standard data provide the level of detail that I need for my application? What happens when the standard data is just not quite right?

Should data translators (filters) be the responsibility of the producer or the user?

6. Recommendations

There is no easy solution to the standardization of data and data systems. It is going to take some hard work and cooperation from all agencies in DoD. The group made the following suggestions to help to ease the process.

- Use incentives. Continue to provide funding only to those organizations whose projects promote and are compliant with DoD standards. Organizations must recognize the value added to data sharing.

- Start standards at the data producer level. The standardization of data has to start at the producer level. It is here that the data are created and so should be the rules governing that creation. If the same type of data is also created at other agencies, it is the functional data administrators responsibility to arbitrate a set of standards.

- Categorize the data that needs to be standardized. The focus for standardization efforts should be based on a taxonomy similar to the one used by DMSO to define the Authoritative Data Sources.

- Prioritize data categories for standardization. Since everything cannot be completed at the same time, the group suggested the prioritization of the data categories. The priorities were based on frequency of use by the M&S community, the risk involved in trying to standardize something that may not be adequately represented in existing databases, and the resource costs.

- Aggressively pursue opportunities to share data. The more things that are shared the less amount of

resources need to be spent on developing and maintaining redundant data.

- Continue to educate organizations on the benefits of standardizing. It is important to continue working groups, symposia, news groups and conferences that pertain to data standardization. These forums provide an excellent vehicle for information sharing.

CHAPTER 4

EMERGING TECHNOLOGIES

Mr. Steve T. Boyd, Chair and Mr. Mark H. Ralston, Co-Chair

1. Working Group Objectives

Key Focus: The Key Focus was to look at how the emerging and potentially emerging technologies in computer science which impact simulation data and its management within the Department of Defense. This must enable the Department of Defense to better organize, train, and equip so as to better project the Military Services as one part of the overall national security strategy of the United States.

Examine: What are the current tools and techniques to find, access, and retrieve database and model data, standard data elements, and complex data types? Are object oriented data base management systems available for DoD modeling and simulations? Address use of Commercial Off the Shelf (COTS) Software, data search engines and artificial intelligence. How is redesign accomplished with respect to re-engineering and legacy issues. How will the National Information Infrastructure (NII) impact on SIMDATAM? This working group addressed the feasibility and utility of the formation of a DoD-level Data Technologies group.

2. Conduct of the Working Group

Agenda
Tuesday
Examine the Cultural and Political Changes Caused By Technologies Emerging in Computer Science
Technology for Multi-Level Security
Data Rates, How Much, How Fast, Who Cares?
Modeling Analysis, Simulation and Training (MASTR) Data Base and Study Management System, by Steve Boyd

Wednesday
Data Storage and Retrieval
OpenROAD & OpenINGRES, by Dan Hogg
Synthesis, discussion of impact of changes
Break for Lunch
Overview of Change in Computer Science
Present results and conclusions in plenary session

3. Presentations

The Modeling, Analysis, Simulation and Training Data Base Management and Study Management System (Mr. Steve Boyd, Air Force Studies and Analyses Agency.)

After an overview of the functions and roles of AFSAA, Mr. Boyd described the requirement for analysts in AFSAA to perform studies about particular weapons systems or enhancing technologies more quickly, to use models with differing levels of abstraction during the course of the study, and to create acceptable results and present the results in an acceptable style, and then start immediately on the next study with little or no time set aside to actually write the 'after action report' that should accompany the study when it is

placed in a library. As a consequence many of the AFSAA studies contain assumptions which cannot be addressed because of a lack of representative background material. In addition, the senior leadership seems to be requiring more and more detail in the analyses of campaign level issues, to ensure the results of the study will adequately represent the components of a new or suggested new system in the battlefield. This causes much more work to be done by the analyst to locate the requisite detailed data about the system in question and ensure the system is adequately modeled in the more and more abstract models. Since there have been several personnel cuts in the last four years, AFSAA is trying to do more work, in more detail, with less staff, and almost no support staff to help in the presentations and final report process.

A Data Management Process Action Team (PAT) was formed in AFSAA, and used this opportunity to examine the processes of data acquisition and data aggregation or data disaggregation. These procedures seemed to take up much analyst time, and it seemed to depend on a large portion of analyst personal knowledge, that was not easily or regularly documented. It seemed like the most logical place to look to save time. To do this, the PAT created tools to establish meaningful transformation processes to 'convert' source data into 'model data'. The PAT established that the following conditions described the current situation to satisfy customer requirements:

- Quick turn around is required.
- Study manager is responsible for data and prepared to defend the data.
- Knowledge of the data collection lost when study manager leaves.
- The processes of data analysis and study analyses (with models and data) have many functions in common.

The PAT also addressed the internal requirement to create some automated tools for data standardization for models requiring different levels of abstraction. The external requirements, from DISA and DMSO and Air Force instructions and directives to standardize data and data elements in a DoD wide process.

The solution became evident. Within the current technologies of data flow, data storage and computer speeds, a data management tool, called MASTR was developed. As the system is being implemented, the current infrastructure (i.e. data flow in the current network) was discovered to be inadequate. Changes in the Local Area Network (LAN) are underway to accommodate these problems. The MASTR process created a single set of tools for data and study analyses, and allowed limited access by the action officers to 'pull' appropriate data for their studies, and allow the data analysts the ability to create new data sets for use by the study analyst/action officer. The system seems to be working quite well. Not all features in MASTR are being used by the study analysts.

Open Road and Open INGRES (Mr. Dan Hogg, The Joint Staff J-8 ASD)

Mr. Hogg presented an overview of the market strategy of a company called Computer Associates. The company is creating data management tools that will be available, useful, and transportable across a wide range of computer platforms and data repositories, from very large data sets, as found in commercial banking accounts, down to fairly small data applications on personal comput-

ers. The Company desired to create a customer base at all levels, and acquired the INGRES Corporation in order to add the PC and engineering workstation data management tools to their customer base. In this process, they took INGRES, which previously chose not to make their tools interface with other data base management systems, and spent $300,000,000 to change INGRESS functions so that it could incorporate or address many of the current and anticipated data base management systems that are on the market. In addition, they chose to increase the capability of the 'packaged' application development tools that are associated with the Computer Associates line of products, including INGRES. They intend to market those application development tools to create interfaces to customer databases that are responsive to the immediate customer needs. Rather than making a revolutionary change to a fundamentally relational data base management system structure, they created an Object Oriented Design (OOD) interface to the currently used relational data bases. This allows objects (of whatever nature) to be stored as elements in a relational data base, but not demand a significant shift to the development and re-engineering of data bases that are already implemented and are heavily invested in the market. The speed of computers, increased flow rate and increased storage allowed CA to build an interface to 'OOD' rather than re-design the total process.

Mr. Hogg described these processes as they might impact the design and utilization of military data base management systems for modeling and simulation. He is very aware of the difficulties in obtaining data that is adequate to the analysis tasks to which the action officers in the Pentagon (and elsewhere in the military community) have been set, and described a software package which would make the implementation process much easier.

4. Discussion

The group met to discuss enabling technologies in the arena of increased data flow (i.e. increased compression and bandwidth), increased computer speed (i.e. faster chips, massively parallel processing), and increased storage (i.e. faster hard drives, flash memory, other schema to compress, store and retrieve data).

The overall discussion seemed to relate to how each service or how each company does its business; rather than on the tools they use to do the business. Within the marketplace, and within the executive branch of the U. S. Government, changes seem to be taking place, whether or not we are ready, or whether or not we understand them. The changes are taking place because of the 'enabling technologies' not because the business and executive branch structures desire the changes or even can control them. The technology of data flow and information flow has changed instantly how senior leadership (military, government civilian, or industrial,) perceives the value and timeliness of information. The television cameras, which looked on in Vietnam and was delayed in its transmission to the 'public', was already in place in Kuwait and Iraq during Operation Desert Shield and Operation Desert Storm. Satellite feeds to the commercial world were functioning at all times, it seems. CNN supplied bomb damage assessment; CNN supplied very emotional scenes which swayed public opinion wherever in the world the 'public' saw the images. The creation of a network of information that flows world wide at near or at real time is changing

the expectations of senior leadership on what they want to have available to organize, train and equipe their forces for war, and indeed, on how they intend to prosecute a war once it has started. Intelligence data is valuable, but its value is dependent on very many factors, and most of them cannot be quantified easily. Old data are not useful to prosecute a war, but are useful to examine how a war might be prosecuted. It is undisputed that Desert Storm Theater of Operations used CNN to do bomb damage assessment for them. However Desert Storm also did not want CNN to know, display or even speculate about how Gen. Schwarzkopf intended to prosecute the war. At that point, the characteristics of the equipment was not at issue. A warrior must have the capacity to strike at the enemy's weakness with strength, and to cause the enemy to put his strength at the wrong place, and do this in secret; this is at issue. The flow of data and communications makes this task more and more difficult all the time. The very same enabling technologies which allow us to 'do a better job' may also cause a downfall for the same reason.

In the world that uses models and simulations for analysis, the primary question came to be 'How can I meaningfully implement these technologies?' not, 'What technologies can I implement?' The military service representatives,the DoD representatives and the commercial industry representatives (without attribution, of course) seemed to agree that the institutions for which we work desire to hide more than they desire to share and that they desire to obfuscate more than they desire to clarify, unless it is clearly to their advantage to expose or clarify. Like a war that takes place on television, the increased flow of information causes a decrease in control, and a potential loss of personal or organizational power. The power loss is feared most when there is not a shared view of purpose. The goals of individuals and individual organizations (without attribution) may not be the goals of their parent organizations. The technological shift toward centralized or distributed access to data, to make available knowledge that once was hidden and personal will change forever the way by which a management or organization can expect to do business.

5. Issues

The primary issue revolved around how the enabling technologies in computer science can be implemented.

6. Recommendations

This group has several recommendations which will allow the enabling technologies to enhance the power and utility of models and simulations in the military environment and minimize the negative effects such technologies may have.

- A strong emphasis should be given to distributed data storage, distributed processing and a wide dissemination of analysis results back into the 'community' into which the data capacity and processing capability is found.

- Commercial Off The Shelf (COTS) software should be used wherever possible for the management and manipulation of data; there is little or no value added in trying to create 'special purpose packages' to perform the business of data administration and dissemination. The embedded software of weapons themselves would continue to be 'developed' packages.

- A DOD level Data Technologies group should not be established, but that the DISA and DMSO organizations be reminded of their charters in that area.

- MORS should establish a working group on Cultural Changes which will enable the Military OR community to more purposefully do the analysis and make the recommendations that will enhance our power as a powerful nation and will decrease the negative impact such technology may have on the community.

CHAPTER 5

DATA SECURITY

Ms. Janet Y. Morrow, Chair and Ms. Lana E. McGlynn, Co-Chair

1. Working Group Objectives

Key Focus: What are the solutions to the data security and classification issues?

Topics for Examination: What are the issues associated with security classification of data? How can M&S security requirements be addressed?

2. Conduct of the Working group, Agenda and Speakers

Tuesday, 28 March 1995.

TOPIC: What are the security requirements associated with Modeling and Simulation?

Identify key issues.

SPEAKERS

Darryl Warfel - Defense Information Systems Agency, Center for Information Warfare:
"Threats to the Defense Information Infrastructure"
Russ Flowers - Network Security Group, National Security Agency: "Data Security Working Group"
Rob Wright - Resource Consultants Inc: "Industry Concerns Regarding Information Exchange for M&S"
Annette Ratzenberger - National Simulation Center: "WARSIM 2000 Security Requirements"

Wednesday, 29 March 1995.

How can M&S security requirements be addressed?
Rebecca Bace - Division of Infosec Computer Science, National Security Agency: "A Real World View of Computer Security"
Donald Marks - National Computer Security Center: "Fundamentals of Data Security"
Darrel Sell - National Computer Security: "Available Security Products"
Terry Mayfield - Institute for Defense Analyses: "High Level Architectures and Security Concepts of Operations"

3. Presentations

Threats to the Defense Information Infrastructure. This very informative briefing identified threats to the defense information infrastructure. It included an explanation of what intruders have done in the past, such as, destroying data, modifying software, stealing data, shutting down hosts/networks, stealing software, modifying data, and destroying software. Multiple intrusion techniques have been used including running automated attack application for Internet Protocol (IP) spoofing attacks, sniffers, back door logins, stealth diagnostic tools, and use of vendor diagnostics. Intruder tools are available over the Internet, in public magazines, and on other mailing lists. Intrusions are often invisible, and may leave systems vulnerable long after the intruder has de-

parted. Vulnerability assessments have shown that 88% of DoD unclassified computers are "easily" penetrated, 96% of these penetrations were undetected by the host administrators and users, and 95% of detected penetrations go unreported. In order to combat network intrusions, system administrators need to know their systems inside out. One recommendation brought out was that system administration should be the primary duty for system administrators, rather than an additional duty.

Data Security Working Group. This presentation focused on network security, highlighting requirements analysis. In developing security policy, the requirements analysis process must address critical factors such as mission capability, information value, information flow, and threats/vulnerabilities. There has to be a balance between operational requirements and risk. An increased number of potential attackers/threats, increased knowledge of attack methods, more affordable attack technology, and more lucrative targets due to operational consolidation are just some of the factors that contribute to increased risks. To ensure data security, the approach taken must consider data as they exist in storage, transit and processing forms. In designing the security system, the desired capabilities of the system need to be mapped to specific security services. Currently, DoD is trying to move security out of the lower level communication protocols (which require DoD to own/operate dedicated communications networks) and instead move security more into the local system environment, thereby allowing for the use of public switched networks. The transition will take time and will necessitate use of suites of systems and mixtures of products such as FASTLANE, crypto cards, trusted applications, secure network servers, firewalls and inline network encryptors until appropriate strength end-systems are fielded. Just what is required is a management decision as well as a security issue, but ultimately the need is still a good security management infrastructure.

Industry Concerns Regarding Information Exchange for M&S. This briefing identified four main industry concerns that should be addressed in line with the recent DoD emphasis on streamlining and reducing the cost of data and information in acquisition:
1) electronic transmission of proprietary data,
2) standards for transmitting digital data,
3) government hardware/software, and
4) handling classified data.

As we look at these areas, we need to address the details in order to develop requirements. Solutions to these and other concerns can be reached through close cooperation between industry and applicable Government agencies. The Government needs to articulate its desires and objectives and provide guidance to deconflict policies and procedures that currently hamper full implementation of Continuous Acquisition and Lifecycle Support (CALS) and the use of commercial standards across Services.

Industry needs to work closely with the Government and academia to take the Government's intended outcomes and derive strategies and tools to accomplish these objectives.

WARSIM 2000 Security Requirements. The central theme of this presentation was that "Not every soldier has a security clear-

ance, but every soldier must be trained." In order to meet training requirements we must get away from the domino theory view of data classification and move toward a seamless synthetic environment. The use of classified data should be based on the question "what can be derived from the application of that classified data in a modified state?" If classified data cannot be derived, then can we use the modified classified data to support an unclassified training application? The idea is to broadcast the enumerated state, not the classified data. The follow-on question then is how do you transmit the enumerated state across systems or nodes at the lower classification domain level? In order to answer these questions and create the seamless synthetic environment, we must start by defining the requirements. The roles of the soldiers and other simulation participants are a taxonomic key in articulating the information protection and information sharing needs.

A Real World View of Computer Security. This presentation provided additional information on threats to computer systems and the impact of intruders. Today, computer systems are vital, and the more interconnectivity, the more complexity we must deal with in designing security. A lot of myths abound, and there is little understanding of threat. How can you investigate what you can't detect? The primary problems are still human. We must provide incentives rather than disincentives for people to report intruders and create the prevention measures necessary. Inside intruders are a bigger problem than outsiders. Perhaps one key to solving this problem is to characterize these threats as personal risks instead of official threats.

Legal statutes/codes and rulings lag behind the times. Added emphasis is needed for system management. We also need to work with industry manufactures throughout the development cycle, because system development from concept to full operational capability is currently only approximately 9 months.

Fundamentals of Data Security. This briefing provided not only a wealth of information at the tutorial level but additionally established the state-of-the-art in computer security and identified some key security issues for M&S. Presently, the community is not very far along in addressing distributed computing security problems. Even PC security problems have not been solved. Compartmented mode workstations (CMW) are good for keeping honest people honest; a CMW security violation would be known to be deliberate. Structured walkthrough and other formal review procedures are another approach to ensuring a good software design. Formal decisions need to be made regarding such issues as who can enter data, what can be entered, who can get into the system, and how they can get in.
Role-based access control seems to be the most suitable approach which can be strengthened by the establishment of rule-based access control. Other security decisions should be what software sources are acceptable, who performs system functions, and how policies will be enforced. Multilevel security systems (MLSs) or databases can limit access based on level of clearance. Intelink[1], for example, makes no discrimination as to need to know. Trusted Computer System Evaluation Criteria (TCSEC) has established data labels (really on the data container, not the data itself). A vendor consortium, The Object Management

Group, has established the Common Object Request Broker Agent (CORBA), and is in the process of evaluating requirements and implementation proposals to provide security in CORBA-compliant systems. Such systems will provide standards to pass data between object-oriented elements in heterogeneous distributed systems.

Available Security Products. It is critical to manage the risk that occurs when there is a means for a vulnerability to be attacked by a threat. Threats can be both internal and external. Cryptography can protect both files and communications. Password schemes, PCMCIA cards, and biometrics are means to establish authentication and identification. Various data bases have been certified for MLS. New secure operating systems are being evaluated at higher levels of trust, and more are coming. Other products, such as firewalls and routers, will add security measures on the network. It is strongly advised that evaluated products be used to ensure one is getting the protection advertised.

High-Level Architectures and Security Concepts of Operations. The Defense Information System Security Program (DISSP) is focusing the direction to be followed in securing information systems. In the future, DoD information systems must be sufficiently protected to allow connectivity via common-carrier communication systems. Additionally, DoD information systems must be sufficiently protected to allow distributed information processing among multiple hosts on multiple networks in accordance with open systems architectures. Information systems must support information processing under multiple security policies of arbitrary complexity, including those for sensitive unclassified information and for multiple categories of classified information. They must also support distributed information processing among users employing resources with varying degrees of security protection, including users of non-secure resources, if required. These DISSP goals parallel requirements for M&S distributed applications. The Defense Goal Security Architecture (DGSA) provides the vision, concepts, and engineering framework by which these goals can be reached. It provides the "security road map" for system security architects. Key among these are the concepts of information domains, strict isolation, security contexts, and security associations. The concepts provide the basis for encapsulating data and securely transferring it within and between individual end sytems.

The DMSO Advanced Distributed Architecture Working Group's "High-Level Architecture" (HLA) for M&S provides important concepts and rules which can be used to align M&S data security with the DGSA. Conceptually, each simulation may consist of one or more information domains spread across the simulation exercise space. The HLA concept of operations (CONOPS) provides data exchange rules that help define top level data security requirements. The HLA rules align nicely with the DGSA "rules" for information domains, security contexts, and security associations. The HLA structure allows each exercise proponent to work deeper into data security problems using a consistent framework. In continuing the DMSO data standardization and security efforts, it will be useful to begin to identify and structure information domains within the context of the HLA, and incorporate information domains into specific simulation exercise plans.

4. Discussion

Security Requirements

Participants identified general overarching security requirements:

- DoD requires simulations wherein participants operating at various levels of classification can interoperate on a battlefield composed of live, virtual and constructive components.
- Disparities in perception of the battlefield among the players imposed by security restrictions must be identifiable and accounted for in interpreting the results of simulations.
- It must be possible to modify simulation data to various classification levels based on simulation requirements. Use of reclassified data must not result in negative training, high cost, or mandatory clearance of personnel not normally cleared.

Protection of information must include not only issues of national security but also the protection of proprietary data. The Government must develop policies, procedures, and provisions in the Federal Acquisition Regulations and the Defense Federal Acquisition Regulations that will provide adequate safeguards for contractors when proprietary data must be delivered. It is unacceptable to require the contractor to prove that the proprietary data have been compromised. It is unacceptable to require the contractor to prove that the Government lost control of the data with the result that the proprietary data were made available to other contractors for their use without proper notification and compensation to the originating contractor. Review of the data requirements and the resultant streamlining of deliverable data may solve this problem by permitting contractors to deliver only the data needed to verify, operate, and maintain the product. This could be accomplished to some degree by requiring that all deliverable software be developed from its inception as reusable software and cataloged in a reuse library. Perhaps industry could be given an incentive to populate and use this repository (which already exists). Industry must carefully review and understand exactly what information the Government is requesting, should ask for guidance on unclear issues, and should challenge requirements that don't make sense. Intellectual property rights are defined in FAR 52, 227.4, Rights in Data, as well as DoD 5000.2, which protects technology from concept formulation through the post-development phase.

The U.S. military is faced with a significant threat and risk as it attempts to use commercially available communications and software. Though untrained "hackers" are able to penetrate systems with relative impunity, the trained foreign operatives who would be well funded and motivated must be viewed with even more alarm. Any network connection to an uncleared network such as Internet will cause positive system attacks from hackers and render classified data vulnerable. It is therefore necessary to install serious security measures to protect M&S systems and data. A layered and comprehensive approach to security is needed. For example, if an unauthorized person gains access to the computer system, that alone should not allow the person to access classified data. The most viable means of accomplishing this goal is through the use of secure operating systems, data encryption, and multilevel secure data bases. These mechanisms may be used to prevent read or write capability and to ensure that critical files and information remain unadulterated. Im-

proved security practices of Identification and Authentication as well as improved data integrity are required to minimize the threat of attack. Risk analysis should be performed to compare the threat against system requirements. MLS systems must use data labeling to ensure data separation.

Simulation exercises are often federations of various interest groups, uniquely bound together by a mission-oriented security policy for the duration of the exercise. The Defense Goal Security Architecture (DGSA) defines each special interest group as an Information Domain (ID). The interaction across these IDs is also mission driven (i.e. the policies and procedures for exchange of information are determined by the value/risk of the ID and its contribution to the mission). Interest groups that have the responsibility for interacting in some larger federation must explicitly define in mission terms their requirements for information exchange. These requirements will be translated into security policy and specific data transformation requirements that enable information to be moved from one domain to another.

The requirements will also be used to identify domain attributes that establish a new "federated" information domain. The DGSA provides two concepts in particular that help in understanding this information exchange process, namely the concepts of a security context and a security association. The concept of a security context is useful when building an information domain based on the end-system resources in which it will execute. The concept of a security association is necessary when negotiation across end-systems is needed to ensure that the ID is properly preserved and protected in the security contexts of two or more end systems. The DGSA also has certain high-level rules on information exchange between security contexts and security associations. One rule is that in order to move information between IDs, the member executing the move must be a member of both IDs. A second rule is that information transferred among end-systems can only be transferred within the same ID. To illustrate this federation data exchange, consider a simulation data base containing sensitive (enumerated) performance data, which is used to support a simulation training exercise consisting of heterogeneous infantry, air defense, and armor simulators. The high-level architecture for advanced distributed simulation has provided the concept of individual simulations joining with, operating with, and retiring from a simulation exercise. The basis is a negotiated set of protocols that provides for behavioral state exchanges. Thus if a simulation component that synthetically calculates an aircraft's interaction is added, the component will use specified protocol data units (PDUs) to provide behavioral state data to the federated simulation. The state data are calculated within the sensitive domain. Using explicit desensitizing transfer rules, the "desensitized" data are then moved into a new, less sensitive domain, which creates the PDU and then sends the PDU to the federating infrastructure for distribution to other appropriate participating simulators who have membership in the desensitized ID. Data flow across IDs is one way in this case.

It must be possible to "Train as we Fight"; i.e., it must not be necessary either to give security clearances to all soldiers so that they can train, or to restrict training to unrealistically general levels of information. Future training environments will provide a

realistic, seamless, synthetic battlespace for training in both individual and collective tasks. In today's distributed simulation environment, the exercise is typically run at a system-high level of security.

For example, if one input is classified, the single simulation/model is considered classified, which then forces the node to be classified, and in turn forces the entire exercise to be either classified or segmented. During Atlantic Resolve 94, the Aggregate Level Simulation Protocol (ALSP) confederation of models was run as a classified exercise. The Synthetic Theater of War-Europe (STOW-E) was run on two networks — one classified (USAF and USN simulations, simulators, and live) and one unclassified (USA live, virtual, and constructive). Objects on the classified net were able to "see" and "shoot at" objects on the unclassified net. However, the objects could not kill objects in the unclassified world.

Training audiences are composed of all ranks, MOSs, skill levels, and levels of security clearance. Not every soldier needs a security clearance in order to perform his wartime mission. Yet, every soldier must be trained in a realistic training environment. Furthermore, soldiers with different levels of security clearances must be able to train TOGETHER in situations comparable to the real-world conditions and real-world security requirements. Use of a model or simulation should not introduce more stringent security requirements. The following is an example of how simulation induced tighter security controls.

In the real world, a tank crew member may observe a fixed-wing flight and a munitions firing. Live exercise participants are not required to have a security clearance. However, if that same tank crew member observes this same phenomena in the virtual world, he is required to have a clearance because the aircraft flight characteristics are classified and these characteristics are used in the calculations of trajectory, probability of hit, etc. There should be a means for determining the security classification of the visual/graphical portrayal to which the crew member is privy. And in many cases, the graphical portrayal could prove to be unclassified. This discussion leads to risk issues of the aggregation of unclassified data, e.g. single instances of an aircraft location, and the ability to infer classified performance parameters from a sequence of graphically-displayed aircraft locations in limited-view simulators.

In developing security policy, the requirements analysis process must address critical factors such as mission capability, information value, information flow, and threats/vulnerabilities. There has to be a balance between operational requirements and risk. An increased number of potential attackers/threats, increased knowledge of attack methods, more affordable attack technology, and more lucrative targets due to operational consolidation are just some of the factors that contribute to increased risks. To ensure data security, the approach taken must consider data in storage, transit and processing forms. In designing the security system, the desired capabilities of the system need to be mapped to specific security services as shown below.

DESIRED CAPABILITY	SECURITY SERVICE
Protect information from:	
-Unauthorized disclosure	Confidentiality
-Unauthorized modification	Integrity

Protect processes users from:	
-Forgery, masquerade	Authentication
-Falsely denying participation	Non-Repudiation
Protect system from:	
-Denial of service	Availability

Solutions

The Defense Information System Security Program (DISSP) provides a means of charting the course to be followed in securing information systems. DISSP addresses questions as to where we need to go (goals), what is needed to get us there (requirements), what these future systems might look like (architectures), and how we can map a route to realize that vision (transition planning). Through a process of information security system engineering, the Defense Goal Security Architecture (DGSA) provides a framework for achieving the vision. Principles have been identified. Concepts have been defined and studied. Relationships among dimensions of the problem have been recognized. Research and development areas to get to implementation have been identified. The establishment of this overarching program and development of this comprehensive engineering approach show tremendous potential to achieving the security objectives that we need.

The Multilevel Information System Security Initiative (MISSI) is another hopeful sign of future improvements. Although there is still some indecision as to whether M&S interoperability requirements can be achieved without complete realization of MLS networks, MLS databases, and compartmented-mode workstations, there is no doubt that M&S requires support from multi-policy systems; i.e., we need the ability to combine all information systems into a single, integrated system that can separate information at any classification or sensitivity level. Advances in technology at the data base, system, and network level would make achievement of this goal easier.

There are hopeful signs that the Common Object Request Broker Agent (CORBA) will provide a common framework within which object-oriented security needs can be addressed. The OMG has included security as a requirement.

Although security was not specifically addressed in the most recent High-Level Architecture development discussions, the current draft architecture conveniently provides hooks for overlay of a security architecture. In the future, at least the need for a framework on which to impose a security architecture should be overtly recognized.

It would be naive to expect the development of a magic bullet or technology which would mitigate the need for a comprehensive model, simulation and data security program. A layered set of technologies is required. Products are in development. Improvements are on the horizon. Nevertheless, for the foreseeable future, security issues will impede achievement of the fully interoperability M&S environment that is so necessary. Conscious decisions must be made as to the level of risk which is acceptable in order to achieve the benefits of fully interoperable M&S.

It may be possible to adopt a phased approach towards achieving fully interoperable simulations wherein M&S components operate under differing security requirements within the same simulation. Presently, a

"system high" architecture requires all M&S roles to operate at the highest level of classification of PDUs traversing the network. However, it may be possible to establish "Secure Partitions" in the simulation. With this approach, one could establish "secure enclaves" which hide their classified data and computation from other players. Information exchange among the players would be restricted to information that could be sanitized, even if computed based on classified data, using classified algorithms, or based on classified capabilities.

The intent would be to use the classified data but hide classified attributes from players without a need to know. There would remain an issue of inference; i.e., whether the classified information or capability could be inferred from the sanitized information which was shared. Such a determination would be simulation specific and should be addressed as part of the simulation design. In the more distant future, a "multi-policy security" architecture incorporating full M&S interoperability among players at various levels would be the ultimate goal.

5. Issues

The vulnerability to attack from within and without on our models, simulations, and data is increasing exponentially. Addressing those vulnerabilities will take a concerted effort. Information on security weaknesses in commercial data bases, hardware, operating systems, and networks is readily available over the Internet, through bulletin boards, and in publicly distributed magazines. Sometimes this information is available as scripts, permitting even the technologically uninitiated to obtain access and information that is deemed private and protected. DoD systems become a more lucrative target as we build large, integrated full-capability M&S and data repositories. As we interconnect our M&S resources in Advanced Distributed Simulation environments, we are increasing the complexity of security engineering and tremendously exacerbating the problems with stand-alone systems. We are only as protected as our weakest link — and today's adversaries are able to scan the universe until they find a single system weak point that permits access. For example, we may build high-assurance end nodes but use protocols which give intruders full access to deny service.

The issues surrounding intellectual property rights extend the requirement for security services beyond protection of classified information in accordance with national security interests. As DoD relies more heavily on contractors for M&S products and expertise, we must assure those contractors through federal acquisition regulations and our proactive and responsible approach to multi policy security that their intellectual property rights will be protected.

Safeguarding the integrity of organizational data needed for program management against internal and external threats is a key issue. Also, we must ensure that our M&S capabilities will be available as needed for the full spectrum of requirements, including operations rehearsal. The Defense Goal Security Architecture has identified a spectrum of desired capabilities and associated security services including identification and authentication, access control, data integrity, data confidentiality, non-repudiation, and availability.

Command emphasis on security is too low. The need for full system security is routinely undervalued, a mistake that has proven very costly in some highly publicized cases in recent months. In one such case, criminals were able to do multimillion dollars in damages in just a few days. In other cases, the losses have been inestimable. Too often management delegates system administration responsibilities to a low-graded employee who may have little training and less authority. Incorporating vendor patches to software may not be given adequate priority, leaving even identified weaknesses exploitable. When security problems are uncovered, management has a tendency to shoot rather than reward the messenger. The false perception persists that intruders are clever ankle-biting hackers rather than common criminals.

The aggregation of models, simulations, and data in an interconnected mode may result in information that requires a higher level of protection. Many issues arise in these situations. At what level of aggregation does the classification change? How can this threshold be detected? Who makes these judgments? This is an issue that must be addressed at the level of the Original Classification Authorities (OCAs) and appropriate classification guidance must be promulgated and maintained within the M&S metadata.

Classified information not discernible from separate modules can sometimes be inferred when models and simulations are connected in an interactive environment. For example, if opposing force battalion commanders consistently suffer a high casualty rate, then it can be inferred that the capability exists to identify and target battalion commanders. Collective simulation results may reveal capabilities that we would wish to protect.

Although data labeling down to the individual element level may be costly, it is necessary to properly transmit and maintain data. To maximize the use of multipolicy security environments and efficiently use transmission capabilities, data elements must be correctly labeled. Merely adopting the classification level of the highest piece of data is not an adequate solution. There is also the issue of sensitivity perishability wherein data may require "re-labeling" as its sensitivity diminishes. The requirement for data labeling also extends to the meta-data level. Certain data users need to the capability to identify the classification authority and the rationale for the classification assigned.

The releasability of DoD models, simulations and data to other Government agencies, to U.S. contractors, and to foreign governments and organizations becomes a critical issue as DoD enters into cooperative development efforts with other nations for the purpose of developing multinational and coalition force exercises. Presently Army is the only service with regulatory policies and procedures for the releasability of models, simulations, and data. Such a policy is needed at the DoD level to ensure consistent handling of these matters.

There are presently several impediments to fully addressing M&S security issues. There is little understanding of the threat. COTS systems may have nuances with implications for security that are little understood. Some commercial hardware may have limited memory management or other design parameters that make it difficult to impose or enforce security measures. Legal and policy regimes lag behind the real-world requirements for M&S security.

Across DoD, the resources for M&S development are shrinking and the demand for M&S technologies is increasing. In order to satisfy the needs of M&S users across all domains (TEMO, ACR, RDA), M&S resources must be applied to build common core capabilities (objects, framework, standards) first. Then only those objects and methods unique to each domain or applica-

tion need to be developed. We must concentrate the security requirements efforts and security tool developments on these key core technologies. Selectable security tools should be the goal.

There is extensive existing security expertise within DoD, FFRDCs, Government Laboratories, and Government Contractors, but without a clear statement from the M&S community as to requirements, the security systems engineers and technologists cannot begin to address our needs. Some overarching security requirements were noted by this working group. However, a comprehensive living document delineating M&S security requirements does not exist. Development of these requirements would focus community efforts on realization of those requirements.

6. Recommendations

Currently, the DIS Vision addresses linking simulations embodying various purposes, technologies, eras, vendors and platforms, but not different security levels. The vision must be expanded to recognize the need for secure M&S wherein participants operating at various levels of classification can interoperate on a battlefield composed of live, virtual and constructive components.

More specific security requirements need to be identified and documented. While we have identified a few overarching M&S security requirements and identified some relevant issues, a continuing open forum for delineating M&S security requirements needs to be established. Without the identification of requirements, there is little chance that the comprehensive solutions needed will be forthcoming.

Command emphasis must be enlisted to ensure the intended benefits of M&S are not compromised through lack of integrity, availability, and confidentiality. If we lose information integrity, we could draw the wrong conclusions from our M&S. If we lose availability, we could lose the critical operational rehearsal tools when we need them most. If we lose confidentiality, our enemies could win the information war. Proper safeguards should not be an afterthought in system development. It must be an integral part of the design process and continued through fielding. These are serious risks that demand the attention of our senior leadership.

We recommend that the DGSA framework be tested on at least one DoD M&S simulation system, possibly STOW-97 or WARSIM 2000. This pilot program would not only provide a real-world test of the DGSA framework, but would establish a programmatic prototype for addressing real-world M&S security needs. Moreover, if this marriage could be arranged at the inception of the M&S development program, means of addressing security could be engineered into the simulation at the outset when they would be most efficient and effective.

There is a need to develop intellectual, engineering, and automated tools to assist in the identification, development, management, and evaluation of security issues in M&S. The MORS community could provide an effective forum for bringing operations research technology to bear in filling this void.

Endnotes

[1] Intelink is an architectural framework and an integrated intelligence dissemination and

collaboration service providing uniform methods for exchanging intelligence among intelligence providers and users.

CHAPTER 6

RESEARCH

Dr. William A. Carpenter, Chair and Mr. Wesley L. Hamm, Co-Chair

1. Working Group Objectives

Key Focus: How can data and data systems be standardized? What are the data requirements and data management implications to achieving dominant battlefield awareness in 2002?

Examine:

- What research is being conducted that will assist in simulation data management?
- What is the latest in data storage, hierarchical storage management, architectures, security?
- What can we recommend for research?
- What are our fundamental unsolved problems in data management?
- What research is being conducted?
- Who is conducting the research?
- What research needs to be conducted to meet the requirements of accessing/using the NII?

2. Conduct of the Working Group

Agenda & Speakers
Tuesday, 28 March 1995
Environmental Effects for DIS (E^2DIS) DMSO Project, Dr. Alan E. Whetmore, Battlefield Environment Directorate, Army Research Lab
Conceptual Data Model for WARSIM 2000 Functional Description of the Battlespace (WARSIM FDB) Prototype, Mr. Oscar A. Chappel, MITRE Corporation
Implementing the WARSIM FDB Class Structure in an ODBMS, Ms. Donna Cornwell, MITRE Corporation
End-of-Day Summary (Group Activity)

Wednesday, 29 March 1995
Report out on ideas resulting from previous day's events (Group Activity)
Automated Repository for Models and Simulations (ARMS), Mr. Carl E. Carden, Integrated Systems Analysis, Inc.
Initial preparation of issues and recommendations (Group Activity)
Combined Arms Tactical Trainer Task (CATTTASK) and Equipment Characteristics Database (ECDB), Dr. Robert H. Wright, Resource Consultants, Inc.
Finish preparation of issues and recommendations (Group Activity)
Working Group Summary Presentations and closing Remarks

3. Presentations

Environmental Effects for DIS

Dr. Alan Wetmore discussed the Battlefield Environment Directorate's support to a tri-Service Defense Modeling and Simulation Office (DMSO) sponsored effort to examine how can or should Environmental Effects (E^2) be modeled in a Distributed Interactive Simulation (DIS) environment. Dr. Wetmore presented four issues that have been identified to focus the E^2 DIS effort:

(1) How to reach real-time operation

(2) How to deal with varying fidelity requirements
(3) How to synchronize environmental data
(4) How to distribute E^2 processing.

Historically, E^2 modeling has been done at the physics-level using fundamental principles. Although this type of modeling produces highly accurate results, it is extremely CPU intensive and does not support real-time applications such as DIS. The logical solution is to either do the number crunching on a large processor(s) and then distribute the results or to use some statistical approximation of the physics-level models which can support real-time requirements. The problem with distributing the results is bandwidth requirements. On the other hand, the aggregation of such data and models that can support real-time requirements is not a trivial process either. As a matter of fact, this process is not very well understood nor has much effort been devoted to increasing our ability to understand the phenomena associated with the E^2 aggregating process. Near-term solution appears to be curve-fits and table look-ups. Proto-typing is underway to demonstrate proof-of-concept.

A major stumbling block to dealing with varying fidelity requirements is the lack of well defined requirements. The DIS Environmental Working Group is now addressing this problem. The next major effort is to develop measures of fidelity and how to apply those measures. Once these measures are developed, understood, and agreed upon within the community, progress can be made in supporting varying fidelity requirements.

The synchronization of environmental data involves getting the right data and using it at the right time. Key to meeting the synchronization problem is determining whether multiple producers can create compatible environmental data. Once we have compatible environmental data, can we then turn that data into compatible environmental effects? Perhaps some sort of master controller for the environment is needed.

Four options are being examined to meet the need for distributed E2 processing. The concept of a master environmental server has been widely discussed. However, the location of such a server and whether one server could meet the needs of a geographically dispersed training exercise, given bandwidth constraints, are primary concerns. This might lead one to consider multiple environmental servers. Once again cost and location are concerns to be addressed. Finally, the idea of one or servers per training area (partition) is a possible solution. However, the cost and synchronization of this solution must be examined.

Conceptual Data Model for Warfighters' Simulation 2000 Functional Description of the Battlespace (WARSIM FDB)

Mr. Oscar Chappel of The MITRE Corporation presented the status the WARSIM FDB object data model being developed for the Simulation, Training, and Instrumentation Command (STRICOM). Mr. Chappel discussed the purpose, scope, and methodology being used to define the Conceptual Data Model for the FDB Prototype. The FDB will serve as a repository for those physical, environmental, and behavioral phenomena required to adequately represent TRADOC's battlespace operating system (BOS) components and functions that must be represented to produce credible simulations of those functions. The class structure briefed by Mr.

Chappel was developed to contain those descriptions and characteristics of the battlespace functions needed to support system domain and software engineering activities by the WARSIM developers. To achieve this purpose, the FDB class structure provides a structure which is capable of containing and producing descriptions of the following domains and their interactions: human characteristics, systems and materiel, physical environment, organization, and doctrine. The initial scope of the FDB Prototype is focused on the operational requirements identified for WARSIM 2000.

Mr. Chappel summarized the methodology used to define the class structure and develop the conceptual data model which consisted of: surveying existing data sources, to include the system or systems used to store the data; identifying the classes needed to meet WARSIM requirements; conducting an IDEF0 analysis to document these requirements; selecting an appropriate CASE tool to support development of the conceptual data model and generate schema for both an object oriented database and a relational database; selecting an object oriented database product (UniSQL) and a relational database product (Oracle); populate an initial "slice" of each type database; compare each implementation and recommend which one the government should use for the full implementation; and lastly, document all phases of the effort. The Prototype is currently being populated and tested in preparation for a final delivery to the government. Upon completion and documentation of the prototype, the government will select a contractor to implement the FDB.

Implementing the Warfighters' Simulation 2000 Functional Description of the Battlespace (WARSIM FDB) Class Structure In An Object Oriented Database

Ms. Donna Cornwell of The MITRE Corporation discussed the implementation of the WARSIM FDB Class Structure contained in the Conceptual Data Model. This work is sponsored by STRICOM, with operational input from the National Simulation Center (NSC). Ms. Cornwell presented MITRE's recommendations with respect to CASE Tool and database implementation choices for the FDB Prototype. Included in the discussion was the primary criteria used in examining the CASE Tools and ODBMS products. Ms Cornwell then discussed the status of the implementation effort. Thus far, the class structures are complete and a conceptual data model is being "fine tuned" using a CASE Tool (Paradigm Plus). Schema for both the object oriented database product, UniSQL, and the relational database product, Oracle, have been generated and are being tested and refined. Two graphical user interfaces (GUIs) are also being prototyped to support both stand alone and on-line users of the FDB. The focus of these GUIs is on the "cognitive" data contained in the FDB. These GUIs will support verification and validation, as well as development efforts. The methodology, lessons learned, data structure, data dictionary, and software developed are being documented for delivery to the government in May 1995.

Automated Repository for Models and Simulations (ARMS)

Mr. Carl E. Carden and Mr. Bill Burch from Integrated Systems Analysis, Inc. presented a briefing and demonstration of a data repository being developed for the Space and Naval Warfare Systems Command, Modeling, Simulation, and Analysis Directorate (SPAWAR 31). The goal of ARMS is to provide a common repository system for users to

access and retrieve data at multiple security levels for models and simulations in support of the Warfighter. The concept of ARMS is to provide a seamless, single point of access to authoritative data to support warfare analyses. The ARMS objectives are: ensure a reliable source of authoritative data for use in assessments and warfighting analyses; reduce redundant data gathering and distribution efforts; establish a means for electronic distribution to models, simulations, and users in the analysis and assessment communities; and provide centralized configuration control and repository management. Mr. Burch noted that this effort, as with other similar efforts, faces the same set of issues and challenges: minimum data element standardization, lack of documented authoritative data sources, difficulties of implementing multi-level security policies and procedures, and minimizing data collection and production costs.

Close Combat Tactical Trainer

Dr. Robert Wright presented an overview of CCTT and the databases developed to support development of that system. The materiel developer for CCTT is the Simulation, Training, and Instrumentation Command (STRICOM). The database work being done to support CCTT is also sponsored by STRICOM (PM CATT). Dr. Wright described the goal of CCTT and the data requirements associated with the program. Key data requirement categories include: weapon system and equipment characteristics, weapon system performance, doctrine and tactics, military operational specialty (MOS) information, crew/force configuration, and environment. The weapon system characteristics and performance are straightforward, and except for the data standardization and authoritative source issues, no major hurdles exist. however the doctrine and tactics, and MOS information needs present new challenges. These challenges include: data sources; automation (doctrine and tactics information is primarily in hard copy); MOS and unit tasks, conditions, and standards (some automated, some not); and verification and validation of tactics and doctrine representations. Dr. Wright noted that although procedures were developed to support the data needs of CCTT, these are in some cases merely workaround until the Army and its data agencies come into the 20th century with respect to data automation.

Efforts are underway to automate the Army's doctrine and tactics. The CALS program, when fully implemented, will provide electronic versions of technical documentation developed in conjunction with new system development. The cost of automating the huge number of existing, hard copy technical manuals is something the services must come to grips with if automated data repositories are to become a reality. In the meantime, the CCTT program is funding those data automation efforts that are needed to support that program. Since there is considerable synergy between CCTT and other combined arms tactical trainers on the drawing board (AVCATT, ENCATT, ADCATT, FSCATT), those common data elements, as well as source code for similar components, will be shared. The long term goal is to have a single data repository to support all modeling and simulation efforts within the Army.

4. Discussion

The Research Working Group took an evocative approach to the working group. First, we arranged for a sampling of presentations from active practitioners in the Data

Management and Modeling & Simulation communities. Second we opened each of the presentations to ad hoc comments, questions, and interjections from the group. Third, we scheduled group discussions to collect and refocus our individual and group thoughts and to pursue issues posed by or exposed by the scheduled interactive presentations. And, finally, we scheduled group input to the process of developing our response to the working group at large.

The results were rewarding. We came away with a group sense of ownership regarding the issues we raised and research areas we recommended.

While many of the research areas we advocate will be pursued (quite naturally) by the commercial/private sector (we expect the entertainment industry to continue as a leader in this area), the government should consider how it can best finance, direct, or at least influence research in the recommended areas.

5. Issues

The group raised six issue areas that it felt deserved attention. These areas and a brief expansion on each are covered below.

Standardization

The group recognizes that there is a separate working group investigating standardization issues, and wishes to add its voice to the calls for standards. Areas that could be improved by standardization include: data compression and transmission standards/protocols, data naming and data dictionary conventions or mappings, tagging and references, VV&A/C,...

CPU Performance

With the advent of more powerful CPUs (including multi-processor architectures) will come the ability to make real-time use of data that heretofore could not be directly included in real-time simulations. The related issues of I/O performance and memory access must be addressed in parallel with CPU performance.

Bandwidth

One of the major impediments to distributed, cooperative simulations is the need to move large quantities of information rapidly between multiple nodes in a network. Additionally, one of the major burdens on today's inter-networking infrastructure is the quantity of information being moved in day-to-day operations. Increased bandwidth is an absolute necessity for continued growth and advancement in the M&S arena.

Integration and Interoperability

Today, there are many instances of multiple systems which perform essentially the same functions (with minor variations). This means that there are multiple development efforts,, maintenance efforts, and operational & analysis efforts being performed in pursuit of the same goals. If we could find ways to encourage cooperation, interoperation, and resource sharing across different organizations, then to paraphrase Colonel Shiflett, "we could spend our M&S dollars on additional capabilities rather than on multiple versions of the same capability."

Aggregation & Disaggregation

It is often the case that the data available for use in a simulation are not of the appropriate

scale (whether it be time scale, spatial scale, organizational scale, or some combination) for direct insertion into a model. Aggregation (the process of translating data from a smaller scale to a larger scale) and disaggregation (the process of translating from a larger scale to a smaller scale) can not be assumed to be linear processes.

Search and Retrieval Tools

There is much data available for modeling that is not necessarily easy to find, to access, or to retrieve. Improving the users' ability to locate and obtain the specific information they seek in a timely and effective manner will greatly improve the overall M&S function.

6. Recommendations

The group produced a number of recommendations for research. These recommendations are presented in no particular order except for the "natural" order in which they were introduced to the group during our discussions and deliberations. These recommendations together with brief explanations are presented below.

(1) Methods for optimizing data representation, data transfer, and data storage

The group recommends that research be done to find HW/SW/protocols that would optimize the access to, retrieval of, storage of, and use of data. Such research could include data compression, data encoding, and error detection and correction.

(2) Standards for data representation, data transfer, and data storage

Related to the above recommendation is the recommendation that sufficient testing be done to take the subsequent step of establishing standards for representing, storing, using, and transmitting data.

(3) Standards for performing and documenting VV&A/C

Right now it seems that each individual organization has its own requirements, procedures, guidelines, and documentation standards for data accreditation and certification. We believe that testing should be done to establish a universal set of VV&A/C procedures and standards. Such a universal set would ease the burdens of the modelers as they search for data, would help eliminate the need for data providers and database administrators to re-certify and re-accredit data, and would provide a consistent, easily traversed audit trail for data analysts.

(4) Approaches for optimizing VV&A/C

Related to the above proposed research, is the proposal to investigate methods and approaches for optimizing the process of performing VV&A/C.

(5) Standards for nomenclatures, terminologies, and dictionaries

Standardization of (or at a minimum, consistent mappings for) terminology as used in data repositories would greatly aid modelers and analysts. What we expressly do NOT advocate here is any attempt to stall the entire process of data presentation until such time as a "universally" accepted set of terms has been established. We do not believe, in fact, that such a universal set will ever be achieved. Rather, we envision a cooperative process in which terms with clearly delineated and un-

ambiguous uses are first agreed upon, and then a process of cooperative mapping and accommodation would begin to eliminate or at least limit the ambiguities remaining in the "universe" of terms. Examples of the success of this approach abound in the Internet community.

(6) Techniques for consolidating nomenclatures, doing semantic translations, and merging taxonomies

In a vein related to the above proposal, we suggest that work be undertaken to foster the merging of existing separate taxonomies. We expect that the first steps in this area would include a proof of concept in which the principal players would be the "interested" parties from two (or more) organizations having separate (but not disjoint) taxonomies. Early successes could be capitalized upon to generate yet additional successes.

(7) Opportunities for pre-calculating, prestoring, and then replaying complex physics-based scenarios

The group feels that there may be a class of conditions under which it would be possible to pre-compute and store certain "time-specific" inputs to real-time simulations and then to essentially "replay" the stored results for input to the real-time simulation. While the uncertainties of the simulation process would preclude such an approach in most cases, there may be a sufficiently well defined class of conditions under which such an approach (perhaps modified by incorporation of some real-time modifications to the recorded results) would prove effective.

(8) Intelligent agents as surrogates for data transfer

This research area is a bit futuristic, but could offer very interesting capabilities for realistic simulation. The fundamental idea is that a simulation can be viewed as a collection of interrelated events and objects and that "generating" or "playing" the simulation from multiple perspectives can be accomplished by passing only information about the movement, intent, plans, or whatever for the elements in the simulation to surrogate elements at each of the "perspective" nodes.

(9) Distributed data systems and distributed processing

Distributing data and processing across a network offers a number of advantages including the potential for increased performance and increased reliability. While much of the effort today in the M&S community seems to be toward centralization of information and computation resources, distributing (or more properly, not centralizing, since such resources tend to start out distributed) such resources will ease the burdens of data management and data maintenance (by sharing them amongst all interested parties) and will provide potentially greater computational resources to all (by cooperatively sharing such capabilities).

(10) Methods for reconciling differences in units of measure, resolution, and fidelity

It often happens that the modeler cannot find the data he or she wants at the resolution (be it spatial resolution, time-line resolution, organizational resolution, etc...) he or she wants. The result is that the modeler must take data at some other resolution and aggregate or disaggregate it in "some fashion" so that it can be used in the model and produce the appropriate results. This process of ag-

gregation (disaggregation) is not straightforward and what is worse, subtle differences in the approach could produce non-subtle differences in model conclusions. What is needed is research into approaches for dealing with either specific instances of mismatch or classes of mismatch to produce reasonable model results with a minimum of "struggle" on the part of the modeler.

(11) "Experiments" to give analysts a "feel" for how one could/should aggregate data

The group recommends that multiple-run experiments be performed (perhaps focusing on weather effects) using physics-based model inputs and aggregates of model outputs to establish a baseline for approaching the problem of aggregating model inputs to obtain aggregated model outputs.

(12) Use of advanced Internet tools for data access and retrieval

The group believes that the cooperative approach to development found on the Internet has resulted in a number of very useful and broadly based tools. The group feels that the M&S community could benefit significantly from the use of some of the search and retrieval tools found on the Internet today. Selective demonstrations of such benefits (or demonstrations of their non-applicability) would help to bring useful Internet tools into the M&S world.

(13) Construction of intelligent search and retrieval tools

In an area related to the above proposal, we recommend that the M&S community look to the Internet community for examples of search and retrieval tools (and approaches taken to developing such search and retrieval tools) that could be used as the basis for developing M&S specific search and retrieval tools.

(14) Creation of tools for identifying and retrieving mathematical equations and algorithms

As a proposal which adds specificity to the above, we believe that the M&S community would benefit from tools for specifically identifying, searching for, and retrieving equations and algorithms.

(15) Investigations into the "appropriate" use of OO, Relational, and Textual databases

Although most of the data available for modeling and simulation today resides in relational databases, there are many instances in which it could be more appropriate to store certain types of information in either textual databases or object databases. Object databases offer the potential for more easily accommodating the representation of real-world objects as data elements in a database. Textual databases (or even collections of text files) offer the possibility of dealing with text in its "natural" form rather than as disjointed data elements, or as large "blobs". The specifics of "if," "when," "where," and "how" relational, OO, and textual technologies should be applied to existing and future data sets needs to be determined. In this manner, we will have a basis for optimally selecting a database vehicle rather than simply going with the "current trend" or sticking with some "pre-existing legacy system."

CHAPTER 7

SYNTHESIS GROUP

Clayton J. Thomas, FS, Chair; Eugene P. Visco, FS, Co-Chair

1. Overview

This chapter reports on the efforts of the synthesis group. The members of this group collected information from each working group while the groups were in session. Members synthesized the information into the following report. This report is based on the feedback briefing of the synthesis group to the final plenary session of SIMDATAM. Our goal was to identify major issues, which are relevant to the SIMDATAM working groups, and overarching themes.

Our charge led to the Synthesis Group's approach and membership. We revisited the SIMDATAM '93 Synthesis Group's formulation of major concerns, issues and recommendations. We inquired as to which of these are resolved and which are still relevant issues. We looked at what is new.

2. Synthesis Group Purpose & Approach

". . . review and synthesize working group findings, identify overarching issues, and prepare recommendations." (from Terms of Reference)

Members had varied military operations research experience. At least one member was in each of the working group sessions to observe and participate. Members pooled impressions and synthesized general findings. As members of our group, we wanted a diverse set of analysts from different backgrounds and services. We tried to have at least one member in each working group session. When the working groups were not in session, we met and pooled our impressions and observations. We formulated issues which we felt to be overarching and prepared recommendations for our final briefing.

3. An Historical Perspective & Simdatam '93 Revisited

"I am throwing up earthworks round our camp, and if it may have no other use, it keeps soldiers properly employed, though I apprehend I have undertaken too much; but as it is now supposed to be a camp of continuance, either now or hereafter, I could not make the lines less."

-Colonel Stanwix, June 18, 1757 from a camp near Carlisle, Pennsylvania

As more recent historical perspective, but very relevant to our purpose, we reviewed three synthesis group charts from SIMDATAM '93: bothersome concerns, overarching issues, and recommendations. We incorporate their lists in the following three questions, and then ask, as of 1995: What's Being Resolved? What's Still Relevant? What's New (Increasing Concern)?

The following concerns were recorded from SIMDATAM '93:

How do we define data?

Where's the catalog of data sources?
How do we get user-friendliness?
Who pays for VV&C and standardization?
What's the shelf life of a data base?
How do we keep up with

- What's available?
- What's going on?
- What we don't know, we don't Know?

There are fundamental problems of definition and systems architecture. How do we define architecture and data. How can we tag data to indicate quality, meaning, and source? How do we identify sources and catalogs? How can we make data bases more user friendly? Can we make technology transparent? What can be automated? Who pays for all of this?

How soon must we pay again? What's the shelf life of a data base? When will new hardware or software make our data obsolete or incomplete?

How do we know the menu of options and what is going on? How do we keep up with data management? How do we face uncertainty?

The following issues were recorded from SIMDATAM '93:

Complexity

- The world itself, and models and simulations
- Technology
- Data Explosion

Specialization Breeds Communities

- Communication Problems
- Responsibility Problems

Dealing with Complexity

- Extent and implications of standardization
- Accomplishing VV&C
- Sharing—Joint, Integrated, Combined

A primary issue seemed to be complexity of data and data management. Many of us were aware of a modeling and simulation community and a data community. We soon learned of a repository community, a data base community, and a standardization community, It is difficult to fix responsibility and find out who is in charge as the number of communities multiply.

Here are several recommendations from SIMDATAM 93 for the MOR community.

- Use M&S priorities to guide data base priorities
- Design M&S to use available data
- Document data origins
- Revisit/review data standardization/VV&C policies for MOR
- Use a SIMDATAM SAG (Senior Advisory Group)
- In future SIMDATAM meetings, "mix-up" the participants
- Emphasize education on data bases (publications, meetings)

Another recommendation was made to create a SIMDATAM senior advisory group (SAG) which plans special meetings and provides continuity between meetings. The SAG would decide upon definitions and descriptions which are useful to policy makers.

4. What's Resolved

Based on SIMDATAM '95 discussions, it appears that the following areas are being addressed:

- Data definitions, cataloging, data modeling, and user-friendliness (DISA push)
- Shelf-life of data bases
- Specialization items (communicating, responsibility)
- Complexity
- Considering data availability when designing Models
- Documentation of data origins
- Creation of SIMDATAM SAG (Senior Advisory Group)

There has been considerable progress in data definition, cataloging, modeling and providing user friendly software. This reflects an emphasis from the Defense Information Systems Agency (DISA). More people recognize that databases decay over time. Communicating and fixing responsibility are seen as issues. There is more formal recognition of the need to consider availability of data when designing a model. MORS created a SIMDATAM SAG and it played a large part in planning SIMDATAM '95.

5. What's Still Relevant

Based on SIMDATAM '95 discussions, the following 1993 issues remain issues in 1995:

- Who pays for VV&C and standardization
- Data Cataloging
- How do we keep up with changes & current tech
- Complexity
- Use M&S priorities to guide data base prioritization
- Revisit/review data standardization/VV&C policies
- Educating analysts on data management & modeling

Who pays for VV&C and standardization is a matter that services and agencies still answer differently. Data cataloging is one item on which a lot of progress has been made. It is a very important and a deep subject of research. Using M&S priorities to guide the prioritization of data bases for VV&C and standardization have pragmatic and theoretical foundations. Important M&S have a great need for data we can use with confidence. M&S are a useful guide in solving data base problems where a general theory is incomplete.

VV&C, standardization, policy review, analyst education on data management and modeling are important steps which need to be addressed to strengthen our data infrastructure.

6. What's New (Increasing Concern)

Based on SIMDATAM '95 discussions, we concluded that the following are of increasing concern and importance:

- Bandwidth issues
- Real-time computation
- Cost
- Which technologies/databases should be funded
- How should the funding be apportioned
- Multi-level security balanced against interoperability
- Implications of data "ownership"—cost, control, responsibility, maintenance, and security
- Policies for implementing data collection, provision, and certification
- Data modeling growing in importance
- "Metadata as important as data"
- Training/DIS applications increasingly demand data modeling.

The growing desire for larger models and simulations with increasing fidelity and resolution have led to interest in bandwidth limitations and real time computing. Shrinking budgets have increased our concern with costs and resource allocation. We must prioritize resources and attainment of databases. Increasing security at all levels leads to a decrease in interoperability of the systems. The need for a balanced approach is clearer than the means of defining it and attaining it. Interface arrangements and the full implications of data ownership are not clearly defined. Who pays for services, who is responsible for certification and for how much certification have yet to be decided. Security is another thorny problem. Policies for implementing data collection, provision, and certification are needed. Data management is being treated professionally. Demand for data management has come from training applications of distributed interactive simulation. Modeling also brings important benefits to analytic M&S.

7. Overarching Observations of '95 and Recommendations

The defense analytic community continues to face an accelerating growth of data, databases, computers, transmission rates, and storage capacity. While there has been commendable progress in solving yesterday's problems, the community is faced with an onrush of new problems which remain to be solved.

This Synthesis Group report summarized some of the individual concerns, issues, observations, and prescriptions that have continuing and new relevance. These hint at the practical knowledge and wisdom that the community is acquiring. Our overarching observations, however, seek to capture our dominant overall impression of a fast paced, dynamic queue, one that reflects laws of nature we can respect, but know only partially. We asked ourselves how to match the overarching observations with overarching recommendations. As we pondered this question, we found our attempts leading us to the following quotation, which says so well what we thought.

"God, grant me the **SERENITY** to accept the things I cannot change, the **COURAGE** to change the things I can, and the **WISDOM** to know the difference." - *Anonymous*

Glossary of Abbreviations and Acronyms

ACR	Advanced Concept Requirement
ADS	Advanced Distributed Simulation
AFPDA	AF Planning Data and Assumptions
ALSP	Aggregate Level Simulation Protocol
ARMS	Automated Repository for Models and Simulations
BOS	Battlefield Operating System
C2	Command and Control
CATT	Combined Arms Tactical Trainer
CALS	Continuous Acquisition and Lifecycle Support
CCTT	Close Combat Tactical Trainer
CFDB	Conventional Force DB
CIM	Corporate Information Management
CIS	Combat Instruction Set
CMW	Compartmented Mode Workstation
CONOPS	Concept of Operations
COTS	Commercial Off the Shelf
CORBA	Common Object Request Broker Architecture
CPU	Central Processing Unit
DB	Database
DBA	Dominant Battlefield Awareness
DDR	Defense Data Repository
DGSA	Defense Goal Security Architecture
DIA	Defense Intelligence Agency
DIS	Distributed Interactive Simulation
DISA	Defense Information Systems Agency
DISSP	DIS Standard Protocol
DMSO	Defense Modeling and Simulation Office
DoD	Department of Defense
DONMSMO	Department of Navy Modeling and Simulation Office
DQE	Data Quality Engineering
DUSA(OR)	Deputy Under Secretary of the Army (Operations Research)
E^2DIS	Environmental Effects in DIS
ECDB	EC Database
ENCATT	EN CATT
FDB	Functional Description of the Battlespace
FFRDC	Federally Funded Research and Development Center
GUI	Graphic User Interface
HLA	High Level Architecture
IP	Internet Protocol
JDBE	Joint Database Entity

LAN	Local Area Network
MASTR	Model Analysis Simulation and Training
MISSI	Multilevel Information System Security Initiative
MLS	Multilevel Security
MOR	Military Operations Research
MORS	Military Operations Research Society
MORSS	MORS Symposium
MSDS	Master Simulation Data System
MSRR	Model and Simulation Resource Repository
NGIC	National Ground Intelligence Center
NII	National Information Infrastructure
NSA	National Security Agency
NSC	National Simulation Center
OCA	Original Classification Authority
ODBMS	Object Database Management System
OMG	Object Management Group
OO	Object Oriented
OOD	OO Design
OSD(PA&E)	Office of the Secretary of Defense (PA&E)
PDU	Protocol Data Unit
PHALANX	The Bulletin of Military Operations Research
RDA	Research, Development, Acquisition
SAF/SAFOR	Semi-Automated FORces
SIG	Special Interest Group
SQL	Structured Query Language
STRICOM	Simulation, Training and Instrumentation Command
TCSEC	Trusted Computer System Evaluation Criteria
TEMO	Training, Exercises, and Military Operations
TOR	Terms of Reference
TRAC	TRADOC Analysis Command, TRADOC Analysis Center
TRADOCAC	TRAC
TWISTIAC	Tactical Warfare Simulation and Technology Information and Analysis Center
USACAA	US Army Concepts Analysis Agency
USAFSAA	USAF Studies and Analysis Agency
USAMSMO	US Army Modeling and Simulation Management Office
USCENTCOM	US Central Command
USAWC	US Army War College
VV&C	Verification, Validation, and Certification
WWW	World Wide Web

Appendix A

Agenda

Monday, 27 March 1995

1700 - 1800 Early registration

Tuesday, 28 March 1995, (First Day)

0700 -0800 Registration (Coffee, Pastries, Juices)

0800 -0830 Welcome and Opening Remarks

0830 -0930 Speaker one

0930 -1000 Break

1000 -1100 Speaker two

1100 -1200 Speaker three

1200 -1330 Working Luncheon with Guest Speaker

1330 -1630 Working groups

1645 -??? Mixer

Wednesday, 29 March 1995, (Second Day)

0800 -1500 Working Groups (Working Lunch)

1500 - 1630 Working Group Summary Presentations via VTC
Closing Remarks via VTC

Appendix B

Terms of Reference

Simulation Data and Its Management (SIMDATAM)

1. Goal: The goal of this workshop is to examine and make recommendations regarding the context, processes, and technology advances in developing and utilizing simulation data and data management.

2. Background: a. In 1991 the Deputy Secretary of Defense instituted an initiative to strengthen the application of modeling and simulation (M&S) in the DoD community. This increased emphasis has stirred efforts to improve policy, procedures, and techniques in developing interoperability standards and protocols among DoD M&S activities. Promising advanced technologies and investments in improving current M&S capabilities in simulation data and its management must be exploited and promulgated to maximize M&S efficiency and effectiveness. Simulation data management (SIMDATAM) is one of the most critical aspects of M&S. The SIMDATAM series focuses on simulation data development, standardization, transformation, storage, maintenance, and transmission, in an interoperability environment.

b. SIMDATAM 93 was held 16 - 18 November 1993 at Falls Church, VA. It concluded that data base and other technologies have great potential. However, that potential does not come effortlessly or without concerns. These concerns lead to a central issue--complexity, ever increasing complexity, it seems. Models and simulations are more numerous and complex, technology has increased and proliferated, and descriptions of the world have led to a data explosion. This has led to increasing specialization. As we deal with these difficulties, we seek standards, ways of certifying data and sharing. Such approaches offer both promise and challenge--problems that we shall probably solve only gradually. Following are SIMDATAM 93 recommendations:

(1) A V,V&C group should be formed. Group should define terms; recommend policy, procedures and guidelines; define V, V&C processes, and tackle other V, V&C issues.

(2) A standards group should be formed. Group should develop taxonomy, help in deconflicting standards, determine de facto standards, and share information.

(3) As data bases are developed, we should prioritize. Use importance and priority of individual models and simulations to guide data base priorities to include standards and V, V&C.

(4) Ensure that new M&S are designed to use available data.

(5) Develop a standard source catalog. The catalog will document data origins and lineage, include subject matter experts, increases awareness, etc.

(6) Revisit, periodically, policies for data standardization and V, V&C.

(7) MORS should form a SIMDATAM senior advisory group (SAG). The SAG can plan

future workshops, make useful policy input on definition of V,V&C, describing the V&V process, etc. The SAG will provide connective tissue and standing capabilities between meetings. The SAG has been formed. It met on 8 June, during the MORSS at the U. S. Air Force Academy. The SAG's recommendations and guidance are reflected in the planning and preparations for SIMDATAM 95.

(8) For MORS, in future meetings, use even more mixing of participants to encourage inter-community exchanges.

(9) MORS should use its institutions to increase data base education among the members of the Military Operations Research Society. MORS should facilitate the publication of frequent articles in the PHALANX, the conduct of tutorials at the large symposia, and the inclusion of data base related papers both in the symposia and in the new MORS journal.

3. Objective: a. The objective of SIMDATAM 95 is to determine, examine, formulate, and recommend, military operations research standards, procedures, and technology, applicable to simulation data and its management. This workshop will:

(1) Make recommendations regarding SIMDATAM standards and procedures.
(2) Examine and recommend advanced technologies in data management.
(3) Recommend unresolved issues:

(a) Be resolved by the appropriate authority.
(b) Be further researched by the appropriate authority.
(c) Be included for future research by SIMDATAM 9x.

b. Within the framework of goals and objectives, the appropriate workgroups are tasked to answer the following questions:

(1) What is the role of verification, validation and certification in databases and is there feasibility and utility in the establishment of a DoD level standing VV&C Group?

(2) How can data and data systems be standardized? Is there feasibility and utility in the establishment of a DoD standing Standards Group?

(3) What current and emerging technologies would enable the collection, storage, retrieval, and dissemination of simulation data?

(4) What are the solutions to the data security classification issues?

(5) What is the pertinent current research on simulation data and its management? How can it be expedited and applied to current models and simulations?

4. Approach: The workshop will achieve the above goals and objectives through a three-layered approach conducted over a 2 day time frame. The first level is guest speakers and tutorials. The second level is the working group sessions. The final level is the summarization on the second day, follow on sponsor briefings, publication of the proceedings, and articles in the professional media.

a. The first morning will be conducted in plenary session featuring keynote speakers who will address topics common to the entire audience. Topics and speakers are listed below:

(1) KEYNOTE SPEAKER (first hour): To be determined.

TOPIC: The National Information Infrastructure (NII) or SIMDATAM and Operational Issues

(2) SECOND SPEAKER (second hour):

Col James E. Shiflett, STRICOM, Orlando, FL
TOPIC : Setting Data Standards

(3) TUTORIAL SPEAKER (third hour:)

Mr. Roy Scrudder, Computer Science Corp, Ft. Hauchuca, AZ
TOPIC: Data Modeling

(4) WORKING-LUNCH SPEAKER - To Be Determined

TOPIC: Data for Operational Models

b. Working groups will meet in the afternoon of the first day and all of the second day of the workshop. Each working group is encouraged to address all aspects of simulation data to include human performance and behavioral concerns, environmental requirements, and data collection and reduction issues in model input and output. The working groups are:

WG1: VERIFICATION, VALIDATION AND CERTIFICATION/ACCREDITATION (VV&C) IN DATABASES.

CHAIR: Dr. Dean S. Hartley III, Martin Marietta Energy Systems, Oak Ridge, TN
CO-CHAIR: Mr. Howard G. Whitley III, USACAA, Bethesda, MD

KEY FOCUS: *What is the role of verification, validation and certification in data-bases? Is there feasibility and utility in the establishment of a DoD level standing VV&C Group?*

EXAMINE: How can VV&C be expedited and applied to current models and simulations? What is data VV&C? What are the quality issues? What are the certification issues. What are the techniques for VV&C of input data and its associated interaction with methodologies? Can the VV&C of input data be divorced from the source or the methodologies? How does one ensure the quality of the input data? What techniques are being used to do this? What software capabilities and graphics are being used to ensure the data correctly represents

the phenomena intended? What are the issues involving certification and accreditation? What is the difference between the two? This work group will address and make recommendations as to the feasibility and utility of the formation of a DoD level VV&C. The VV&C group would define terms, recommend policy, procedures, and guidelines, and define VV&C processes. Discuss charging this DoD VV&C group with setting guidelines for establishing importance and priority of individual models and simulations. These guidelines would establish VV&C for the supporting data bases. Discuss and make a recommendation regarding the development of a data source catalog, which would document data origins, lineage, and include subject matter experts. Successful tests and experiences with lessons learned are encouraged to be shared between all. Each working group chairperson will render a short verbal report to the entire workshop at the end of the second day. The report will be presented over an interactive inter working group Video Tele Conferencing system.

WG2: STANDARDIZATION OF DATA & DATA SYSTEMS.

CHAIR: Major Walter L. Swindell II, TRAC Ft. Leavenworth, KS
CO CHAIR: Major Karen S. Barland, USAFSAA, Washington DC

KEY FOCUS: *How can data and data systems be standardized? Is there feasibility and utility in the establishment of a DoD standing Standards Group? What are the data requirements and data management implications to achieving Dominant Battlefield Awareness (DBA) in 2002?*

EXAMINE: Current and emerging standards for service data sharing; e.g., standards for terrain database content and transfer format; architectures to interconnect simulations/simulators (e.g. Joint Modeling and Simulation System (J-MASS)); Protocol Data Units (PDU's) for Distributed Interactive Simulations. What are the issues associated with protecting legacy data, standardization of data format, data input and output, SQL? How do we reconcile data standards with major programs? What is the Corporate Information Management (CIM) plan? This workgroup will address the feasibility and utility of the formation of a DoD level standards group. The Standards group would determine the de facto standards, develop taxonomy, and assist in the resolution of conflicting standards. It would issue guidelines on how to promote the use of available data in new models and simulations. Discuss charging this DoD Standards group with setting guidelines for establishing importance and priority of individual models and simulations. These guidelines would establish standards for the supporting data bases. Each working group chairperson will render a short verbal report to the entire workshop at the end of the second day. The report will be presented over an interactive inter working group Video Tele Conferencing system.

WG3: ENABLING TECHNOLOGIES

CHAIR: Mr. Steve T. Boyd, USAFSAA, Washington DC
CO CHAIR: To Be Determined

KEY FOCUS: *What are the enabling technologies that would be useful to the collection, storage, retrieval, and dissemination of simulation data? How would these contribute to Dominant Battlefield Awareness in 2002?*

EXAMINE: What are the current tools and techniques to find, access, and retrieve database and model data, standard data elements, and complex data types? Are object oriented data base management systems available for DoD modeling and simulations? Address use of Commercial Off The Shelf (COTS) Software, data search engines, artificial intelligence. How is re-design accomplished with respect to re-engineering and legacy issues? How will the National Information Infrastructure (NII) impact on SIMDATAM? This workgroup will address the feasibility and utility of the formation of a DoD level data technologies group. The Data Technologies group would monitor the emergence of simulation and data management technology. It would issue guidelines on how to promote the use of available data technology in models and simulations. Discuss charging this DoD Standards group with setting guidelines for establishing the importance and priority of data technologies and with the requirement for disseminating information concerning these technologies. Each working group chairperson will render a short verbal report to the entire workshop at the end of the second day. The report will be presented over an interactive inter working group Video Tele Conferencing system.

WG4: DATA SECURITY (CLASSIFICATION)

CHAIR: Ms. Janet Morrow, U. S. Army NGIC. Charlottesville, VA
CO CHAIR: Ms. Lana E. McGlynn, US Army MSMO, Arlington, VA

KEY FOCUS: *What are the solutions to the data security and classification issues?*

EXAMINE: What are the issues associated with security classification of data? What are the multi-level access issues? Can TCP/IP access permit authorized users to view on-line services while blocking outsiders and unauthorized users? What is the TCP/IP Firewalls Program launched by the National Institute of Standards and Technology (NIST)? Can robust security solutions be developed that meet the requirements of security and the needs of data access? What will the impact of the NII be on data security? Each working group chairperson will render a short verbal report to the entire workshop at the end of the second day. The report will be presented over an interactive inter working group Video Tele Conferencing system.

WG5: RESEARCH

CHAIR: Dr. William A. Carpenter, The MITRE Corporation, McLean, VA 22102
CO CHAIR: Mr. Wesley L. Hamm, The MITRE Corporation, McLean, VA 22102

KEY FOCUS: *What is the pertinent current research on simulation data and its management? Identify the research that will contribute to Dominant Battlefield Awareness in 2002.*

EXAMINE: What research is being conducted that will assist in simulation data management? What is the latest in data storage, data hierarchical storage management, data architectures, security, etc. What can we recommend for research? What are our fundamental unsolved problems in data management? Where is the research being conducted? Who is conducting it; government agencies, commercial entities? What research needs to be conducted to meet the requirements of accessing and using NII data? Each working group chairperson will render a short verbal report to the entire workshop at the end of the second day. The report will be presented over an interactive inter working group Video Tele Conferencing system.

c. Synthesis Group.

CHAIR: Mr. Clayton J. Thomas, FS, AFSAAS/SAN, Washington, DC
CO CHAIR: Mr. Eugene P. Visco, FS, Ofc of the DUSA (OR)
Washington, DC

TECHNICAL ASSISTANT: Major Kevin Giles, USAWC, USAWC, Group Systems V Software

KEY FOCUS: *This group will review and synthesize working group findings, identify over arching issues, and prepare recommendations. Each working group chairperson will render a short verbal report to the entire workshop at the end of the second day. The report will be presented over an interactive inter working group Video Tele Conferencing system.*

5. Membership: The representation is expected to be 50% DoD and 50% industry and academia. Attendance will be limited to a maximum of 100 - 125 persons. Working group chairpersons are considered subject matter experts in their work group area. Membership in the working groups may be controlled by the working group chairpersons. The workshop will be conducted at the unclassified level, however it will be held in a secure facility and security clearances will be required. Security clearances must be forwarded at least one week prior to the conference, to the Commandant, US Army War College, ATTN: AWCSM (Ms. Ann Garman), Carlisle Barracks, PA 17013. The security office phone numbers are; 717-245-3233, DSN 242-3233, FAX: 4433.

6. Products: A briefing will be prepared for the sponsors with specific recommendations within the framework of the focus or each work group. It will report on significant issues, findings, and conclusions. Proceedings will be prepared containing an executive summary, summaries of each working group's report, copies of the text from papers, and textual

summaries or annotated briefing slides. Articles will be prepared for publication in the professional media by each workgroup. Each presenter will prepare an abstract to be included in the published proceedings by MORS. Each working group chairperson will prepare the proceedings relative to his working group.

7. Co-Proponents: The Director for Force Structure, Resource and Assessment, the Joint Staff; The Deputy Under Secretary of the Army (Operations Research); Director of Modeling, Simulation and Analysis, Deputy Chief of Staff, Plans and Operations, HQ USAF; The Director, Assessment Division, Office Chief of Naval Operations; and the Commanding General, Marine Corps Combat Development Command.

8. Planning and Organization Committee Members:

Workshop Chairmen:
Charles E. Gettig, Jr., Chair (SAG MEMBER)
Consultant, Gettig & Associates
3500 Ada Drive, Suite A
Mechanicsburg, Pennsylvania
717-732-9210; FAX: 717-732-6002
E-MAIL:73623.2613@compuserve.com

COL Stephen D. Williams, Co-Chair (SAG MEMBER)
Director, Science & Technology Division
U. S. Army War College
Carlisle Barracks, Pennsylvania 17013
717-245-3165 DSN: 242-3165
FAX: 717-245-3030
E-MAIL:williams@csl-emh1.army.mil
Technical Chair:

Dennis A. Konkel (SAG MEMBER)
Director, Modeling Team A.
Science & Technology Division
Center for Strategic Leadership
U. S. Army War College
Carlisle Barracks, Pennsylvania 17013
717-245-3217 DSN: 242-3217
FAX: 717-245-3030
E-MAIL:konkelda@csl-emh1.army.Mil

Program Committee:
Dr. Erwin Atzinger (SAG MEMBER)
US Army Materiel Systems Analysis Activity
ATTN: AMXSY-DA
Aberdeen Proving Ground, MD 21005-5071
410-278-6577 DSN: 298-6242
FAX: 278-6242
E-MAIL:erwin@brl.mil
Michael Bauman (SAG CHAIRMAN)
Deputy, TRAC
Ft. Leavenworth, KS 66027-5200
913-684-4689 DSN: 552-4689
FAX: 552-3859
E-MAIL:baumanm@tracer.army.mil

MAJ Karen S. Barland
AFSAA/SAN
1570 Air Force Pentagon
Washington D.C. 20330-1570
703-697-5616 DSN: 227-5616; FAX: 703-667-3441
E-MAIL: barlandk@afsaa.hq.af.mil

Mr. Steven T. Boyd
AFSAA
Nuclear Deterrence Division
1570 Air Force Pentagon
Washington D.C. 20330-1570
703-697-5677 DSN: 225-5616; FAX: 703-697-1226
E-MAIL: boyds@afsaa.hq.af.mil

Dr. William A. Carpenter
The MITRE Corporation
W548
7525 Colshire Drive
McLean VA 22102
703-883-5777; FAX: 703-883-3308
E-MAIL: wcarpent@mitre.org

Howard Haeker (SAG MEMBER)
Director, Data Development, TRAC
Ft. Leavenworth, KS 66027-5200
913-684-3030
DSN: 552-3030
FAX: 552-9151
E-MAIL:haekerh@tracer.army.mil

Mr. Wesley L. Hamm
The MITRE Corporation
7525 Colshire Drive
McLean VA 22102
703-883-6403
FAX: 703-883-6143
E-MAIL: whamm@mitre.org

Dr. Dean S. Hartley III
Martin Marietta Energy Systems
Senior Consultant
Data Systems Research & Development
1099 Commerce Park Drive
Oak Ridge, TN 37830
615-574-7670
FAX: 615-574-0792
E-MAIL:dhx@ornl.gov

Mr. Philip A. Kubler (SAG MEMBER)
U. S. Army TRAC, ATTN: ATRC-F
Ft. Leavenworth, KS 66027-5200
913-684-2331 DSN: 552-2331
FAX: 913-684-4368
E-MAIL: kublerp@tracer.army.mil

Dr. Bill Lese (SAG MEMBER)
OSD (PA&E) General Purpose Programs,
Land Forces
Pentagon Rm 2B256
Washington D.C. 20301-1800
703-695-0881 DSN: 225-0881

Ms. Lana E. McGlynn (SAG MEMBER)
U.S. Army Model Improvement and
Study Management Agency
Crystal Square II, Suite 808
1725 Jefferson Davis Highway
Arlington, Virginia 22202
703-607-3385 DSN: 327-3385
FAX: 703-607-3381

Dr. James J. Metzger (SAG MEMBER)
OASD(PA&E)(GPP/LFD)
1800 Defense Pentagon
Washington, D.C. 20301-1800
703-697-7768 DSN: 227-7768
FAX: 703-693-5707

Ms. Janet Y. Morrow
U. S. Army National Ground Intell Ctr (NGLIC)
IANG-RA
220 7th St., NE
Charlottesville VA 22901-5396
804-980-7393 DSN: 934-7393
FAX: 804-980-7699
E-MAIL: jym3k@virginia.edu

Mr. Royce H. Reiss, Jr. (SAG MEMBER)
HQ USAF AFSAA/SAG
Pentagon, RM 1D380
Washington, D.C. 20330-1570
703-695-5552
FAX: 703-697-3441
E-MAIL:reiss@sun19.hq.af.mil

Mr. Roy Scrudder
Computer Science Corp/C4I
Ft. Hauchuca, AZ
602-538-4812
FAX: 602-538-4915
E-MAIL: scrudder@huachuca-emh17.army.mil

COL James E. Shiflett
STRICOM
ATTN: AMCTM-CATT
12350 Research Pkwy
Orlando, FL 32826-6276
407-380-8299 DSN: 960-8299
FAX: 407-380-4201

MAJ Walter L. Swindell II
USATRAC
Data Development
88 Hancock Ave
Ft. Leavenworth, KS 66027-1867
913-684-3030 DSN: 552-3030
FAX: 913-552-3866
E-MAIL:swindelw@tracer.army.mil

Mr. Clayton J. Thomas, FS (SAG MEMBER)
AFSAA/SAN
1570 Air Force Pentagon
Room 1E386
Washington D.C. 20330-1570
703-697-4300 DSN: 227-4300
FAX: 703- 697-3441
E-MAIL: thomasc@afsaa.hq.af.mil

Mr. Eugene P. Visco
Ofc of the DUSA (OR)
Hq Dept of the Army
ATTN: SAUS(OR)
Pentagon, Room 1E643
Washington DC 20310-0102
703-697-1175/0367 DSN: 227-0367
FAX: 703-697-7748
E-MAIL:eugene.p.visco@pentagon-1dms18.army.mil

Mr. Howard G. Whitley III
USACAA
8120 Woodmont Ave
Bethesda, MD 20814-2797
301-295-1611 DSN: 295-1611
FAX: 301-295-1287

Appendix C

Captain Lee Dick's *PHALANX* Article

SIMULATION DATA AND THE NEED FOR STANDARDIZATION

Captain **Lee Dick**, SPAWAR

What is data? One definition which appears relevant is that data is factual information, especially information organized for analysis or used to reason or make decisions. All of the representations captured on the on the collage in Figure 1 are forms of data. Going a step further, information is defined as a collection of facts or data. From these definitions we can focus on three areas; how we collect or gather data, how it is organized or categorized into information, and how its made available for the analyst or decision maker. Let's begin by examining some concrete examples from the user community.

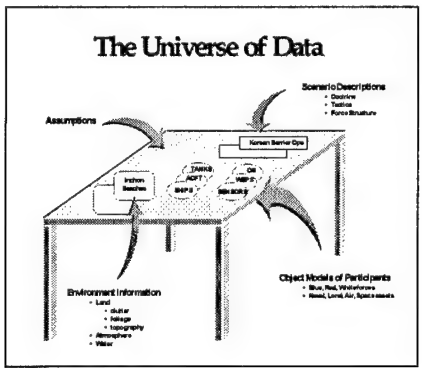

Figure 1

The urgent need for standardized data isn't theoretical nor is it a requirement that will gradually emerge some time in the future. The need is here and it's here now. Perhaps the best and most recent example of what I'm talking about is the Chairman, Joint Chiefs of Staff high level, Two MRC Wargame or Nimble Dancer as more commonly known. It's a well kept secret which fertile mind on the Joint Staff actually thought up that name, but there is evidence to suggest that at least the "Nimbleness" will persist for the future. However, as things have turned out, we can now attest to that individual's foresight and genius.....Nimble Dancing has proven remarkably apropos in describing the data collection footwork we've engaged in to support the requisite Nimble Dancer analysis. The overall Nimble Dancer effort has, in a number of ways, turned virgin soil on the joint collaborative analysis plain.

The questions Nimble Dancer was chartered to answer sound relatively simple. What are the US capabilities and risks involved in fighting the DPG 2 MRC Nearly Simultaneous Scenario...first in the short term - 1997 - and then in 2001 to 2005 with the Bottom Up Review force we're working to field? The answers need not be reported here. Rather what is important was the lack of adjudicated, coordinated, and promulgated data in the overarching effort which comprised all services, OSD and several modeling tools. To reiterate, the level of cooperation between Joint Staff, OSD, all the services, and the CINC's was heretofore unmatched and very impressive. Indeed, as fellow MORS colleague, Mr. Vince Roske, Joint Staff J8, asserted at a Joint Modeling and Simulation Executive Panel last May, "A year ago I would never have fathomed this cooperation". A fact of life is that without such cooperation, what proved to be some eye opening, apples and oranges differences in the characterization and usefulness of the data brought to the table by the different services would have presented an insurmountable task.

Early on in the Nimble Dancer analytical effort, it became apparent that that no one model could support the analytical effort. A process was then developed to collaborate the results of two campaign level models, one which emphasized the ground campaign and the second which emphasized strike and Naval capabilities. As the analysis evolved, so did the process. However, it was recognized up front that data standardization was crucial to integrating the analyses. The vision and progress towards the

development of a joint analytic model of the future will hopefully result in a much cleaner process. But, that effort will fail absent the success of the data standardization effort discussed herein. Moreover, this challenge continues today and will continue to exist until a robust joint analytical model which integrates the capabilities both within and across the services is fully operational. Even with object oriented programming technology, a fully functional, faster-than-real-time simulation which meets all the users needs still may be nothing much more than a pipe dream, particularly when the multi-level security aspects of compartmented and special access capabilities are taken into consideration and, most importantly, if the data requirements to support such a system are not solved.

There were many problems associated with the Nimble Dancer data effort, to be sure, and enormous time and effort on the part of the Nimble Dancer analysts were needed to get as far as they did. The scrubbing of the Nimble Dancer data bases, scenario, and assumptions continued long afterwards. The latter may be the most significant because we all know that understanding assumptions is a crucial prerequisite for the analyst. These assumptions can drive the requirement for data and are, in many ways, themselves part of the data set. The Nimble Dancer action officers hold this as a big lesson learned having spent many hours negotiating the long list of assumptions. Again, this effort has shown us a lot and helped us focus on an area crying for standardized data. The same problems are relevant and the Nimble Dancer lessons learned can or have been applied to subsequent analytical efforts such the ongoing Joint Intelligence, Surveillance and Reconnaissance analytic effort appropriately dubbed Nimble Vision and the recently completed Navy Assessment Division's 2005 MRC/SLOC campaign analysis.

Nimble Dancer is but one example of the need for standardized data. Let's continue with another. The Department of the Navy Joint Mission Area (JMA) assessment process recently celebrated its third birthday while it takes on the challenge of laying the foundation for its second Program Objectives Memorandum, namely POM98. There has been a wide variance in the approach taken by each of the Naval JMAs in developing its own unique assessment. However, it should come as no surprise that those which rely significantly on studies and analysis also place heavier demands on data requirements. Let's take a brief moment to examine the data requirements of one of the more analytically robust assessments, the Intelligence, Surveillance, and Reconnaissance JMA, formerly known in Navy circles as the Joint Surveillance JMA.

One of the key operational capabilities originally defined in the Navy's post cold war strategy "...From the Sea", surveillance is the corner stone which provides the enabling data to conduct warfare. Surveillance is defined as the systematic observation and exploitation of the multi-dimensional battle space by all available sensors. Observations are conducted across the electromagnetic and acoustic spectra in the air, land, sea, and undersea environments. Exploitation includes processing, interpreting, validating and fusing observations and communicating results to decision makers.

The magnitude of data which has to be collected and verified in order to conduct a comprehensive surveillance assessment cuts across a wide spectrum. In its entirety, this list is referred to as a "Common Frame of Reference". Cost and performance trade-offs have to be conducted within the framework of the Common Frame of Reference in order to make a valid comparison between competing sensors and architectures.

It would be helpful if we could reach into one bucket and pull out all the data needed for an analysis effort. However, today that bucket does not exist. Instead, the data effort is very manually intensive and requires that many different experts be physically contacted to collect and validate the data. As an example, one aircraft with different sensors has an expert for each sensor who each must be individually consulted for the correct source of data. In fact, multiple consultations with multiple experts are generally required for total understanding and context. As a result, data collection is a slow, cumbersome process. Many parameters must be checked. Some-

times key data is not available and the expert must be allowed lead time to obtain it. This "gathering" step is only the beginning. The data still requires categorization and user accessibility.

Before moving on, let's elaborate on some of the specific data problems experienced in conducting Surveillance studies from a user perspective. Not only does the data have to cover the complete magnitude of surveillance data requirements, but it must also address differing levels of fidelity. High fidelity models may want it all. For example, they may require a radar to be represented by frequency, beam width, pulse rates, scan rates, power out, false contact rates and countermeasure characteristics, to name a few. However, low fidelity models might be satisfied with search rates alone.

Another data problem often faced is the difficulty in obtaining credible data on potential or projected capabilities as promoted by Program Managers and vendors. Model reruns are required as test results or changed capability projections become available. This is often further complicated by the user himself, as he forces changes in requirements in response to evolving designs and as resources vary. Again, add to that the complexity of systems which dictates multiple experts or sources for a typical combat system. The result is a costly and time consuming data collection and certification effort, which can result in studies not being completed within budget or on time to support their objectives. A verified and validated comprehensive data effort, i.e., the "data bucket", with easy user access could benefit all communities. It would allow shared accuracy, and cut down on redundant, individual data collection. Furthermore, to ensure universal usage, inquiries into data bases must be user friendly, not highly structured requiring detailed knowledge which dictates the services of a support contractor with the requisite expertise.

From an operational perspective, the quality of Surveillance data to the user is determined by accuracy, timeliness and completeness of the data. Command and Control and Information transfer is at the heart of modern "Information Driven" warfare. Delays and massaging of the data as it goes through the links and nodes of the Battle Management Command and Control (BMC2) affect the quality of data to the user. As we move forward into a world characterized by Dominant Battlefield Awareness, the key to coherent joint operations is data management. Technology may well bring a capability see everything and put it all on a Universal Sensor Grid, but how does the right piece of data get to the right party at the right time? One thing for sure, it won't without protocols and standards. Standardization of data should account for effects incurred in data transfer. This situation is further complicated by at least an order of magnitude when integrated with other services to support a Joint Task Force. To that, add interagency/national connectivity and the need to service combined forces. Then on to that add the layering of multi-level security. The point is the movement of data on the battlefield is an enormously complicated challenge and the same architectures and standards which are being applied to manage it may be similar or even the same architectures and standards which govern data required by the analyst.

Last January when Dr. Anita Jones, DDR&E, signed out the draft DoD M&S Master Plan for formal coordination, there was a significant change as compared to the first working level draft back. Namely, the objective referring to architecture was formed into a new objective with three sub-objectives. The last of these three objectives specifically focuses on the data standardization issue. The recently approved Master Plan states that we will establish data standards to support common representations of data in models and simulations and establishes specific actions to meet this objective. This leads to the next example for data standardization, the Naval Simulation System.

The Naval Simulation System is being designed to support the multiple Naval analytical needs from requirements generation and acquisition to fleet planning at the CINC level. As such, it will represent the full scope of theater level warfare. It will cover the broad geographic environment of the theater, and it must represent the various war-

fare areas contributing to the successful conduct of littoral warfare. This is done within a single object-oriented architecture.

Each warfighting system or component that is represented in the simulated battlespace must be based upon authoritative data and verified information if the analysis is to be believed. Much like any other high level architectural candidate, the interaction among the simulated warfighting systems will be controlled by the simulation engine, which must also maintain effectiveness statistics and support the graphical interface providing the analyst a means of interacting with the evolving battlespace scene.

As inferred earlier, the specific data needs of the Naval Simulation System are demanding and cut across a broad environment. The Object Models of Participants require detailed data about system characteristics and operational performance. Environmental information must be provided to support the impact of the various environments upon the operational performance of the warfighting systems. In addition, scenario information and data must be provided about force structures available to each side in the battle, and about the doctrine and tactics to be used by the forces.

The requirement to simulate the warfare at a pyramid of different warfare levels complicates the data problem by imposing the need for providing data at different levels of detail, which implies the need for a consistent way to scale between the parameters at the different resolution levels.

Another view of the role of data in the Naval Simulation System can be expressed by thinking of the system structure in terms of five layers (see figure 2). At the top of the system structure is the graphical interface with the analyst or user. The supporting data must include two or three dimensional maps or charts. The motion characteristics of the simulated platforms must support reasonable trajectories in this space. The analysts must be able to access descriptive information about each platform and its current status in the simulation by "clicking" the appropriate icon on this display.

At the bottom of the system structure is the Foundations Layer which contains the specific databases in which data is stored. This may involve access to remote databases through linkages to necessary networks, including access to live data from fleet communication systems.

A User Perspective Layer is the means by which the particular perspective of the analyst operating the analysis is known and enforced. This is the means by which the operator identifies their particular interest in the problem being run, the particular measures of effectiveness or questions to be asked during the analysis, and, of most significance to the data, the "need-to-know" or clearance access of the user.

An Applications Layer sets up and runs a particular analysis application, depending upon requests passed down from the upper two layers.

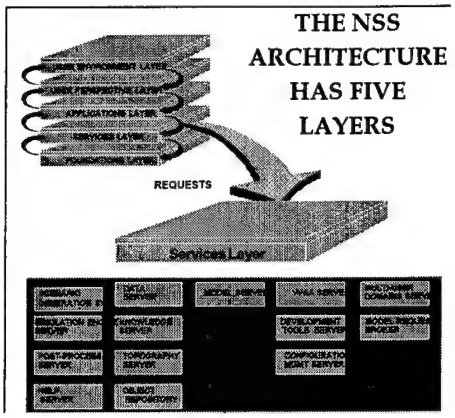

Figure 2

A Services Layer provides key services needed to run the application. Of particular relevance to this presentation is a Data Server which accesses

data in a Foundations Layer in order to instantiate the simulated objects with the appropriate data. An Object Repository is a means to construct the collection of objects being run in the current application for storage in a Foundations Layer to be used for additional analysis later. A Scenario Generation Server is the means by which the analyst is guided through the process of providing the necessary data and information to set up the scenario specific application.

Sound complex? It is and as such demonstrates the enormity of the task that lies ahead. How NSS or, for that matter any model or simulation system, manages the data problem will in the end determine its usefulness. For that reason, the time and attention paid to data man-

agement is time and money well spent.

In summary of the NSS data issues, it should be emphasized first that the data needs to be authoritative. This immediately raises the question of who are the appropriate authorities. The resolution of this question is of primary importance to NSS, and all serious simulation systems. Resolving this should be a task of those responsible for defining data standards.

One of the most significant challenges with respect to data is the shear volume of it. NSS covers the scope of essentially all Naval warfare areas from Space and Electronic Warfare, through Strike Warfare, Expeditionary Warfare, Amphibious Warfare, Theater Air Defense, Mine Warfare and Undersea Warfare, to Command and Control and Information Warfare. Hundreds of warfare systems are involved. And, this is true for both sides of the opposing forces. This is complicated by the need to be prepared for two near simultaneous regional conflicts. Then, finally, the data is required at multiple levels of resolution. Many different databases and resources must be coordinated and ambiguities resolved to prepare the data for such analyses. Hopefully standards can be developed which minimize the multiplicity and ambiguity in the many data resources.

An additional technical challenge for providing data to support different resolution views of the warfare, is the requirement to have consistency. That is, the information that is used as data at the lowest resolution, the campaign level, must be consistent with the information that is used as data when the analysis is conducted at higher resolution, force or engagement level. This is known as aggregation. Technical means need to be developed for aggregating data up to lower levels of resolution. This process also needs to be standardized.

Tactics information is key to the outcome of simulated warfare. There are no standards on how to characterize or implement information about tactics. It is often not possible to distinguish tactics information in a simulation, and the particular means of implementing the use of tactics. Also there are many different tactical situations for which new information must be identified or defined. The Army is making great progress on this through their work on the Functional Description of the Battlespace. ARPA is also adding to this effort with their work on Semi-Automated Forces. This needs to be completed for all the services. Also, the intelligence community has to provide support in this area for threat forces and for potential coalition forces. There is a considerable need for a standardized documentation approach for tactics.

As the Naval services move to warfare characterized in "...Forward From the Sea", there are many different environmental provinces within a single theater, and there is great spatial variation within a given environmental domain such as weather. Also, a given environment has different impacts upon different sensors or weapons. The process of transforming environmental data to its impact upon weapons and sensors must be authoritative from the points of view of both the environment expert and the warfighting system domain expert. This coordination is often difficult to achieve. Standards and Standard Practices need to be defined.

A final point in the NSS data story is the need for fast and efficient database support technologies. We need to have rapid access to existing databases, and we need to have efficient query techniques for reaching into multiple databases to find key information, including the ability to identify and resolve ambiguities.

During a recent visit to CINCPACFLT, the Naval Planning Scenario author was confronted straight on with the data issue. In his report, he stated that "Though the published scenarios were out there, most of the attendees to the briefing had not read the documents and therefore, questions were minimal. What was of paramount importance to the forum, and was the issue, is paraphrased in this quote. "Data bases remain the major shortcoming in achieving a 'Common Frame of Reference' input to the Modeling/Simulation process." Much like the Naval Planning Scenarios have gone through a verification, validation and accreditation process, the large volume of data bases to be applied to the Naval Simulation System requires a

similar process. Only in this way can the objectives of the program be met without being substantially degraded by the 'Garbage In - Garbage Out' syndrome. There is no question about the importance of data and the fact that this was the only agenda item that mattered most in the minds of the vast majority of all "workers" of the NSS initiative. It is and will remain a Priority ONE issue.

Where does it all lead? In his address to the Association of Modeling, Planning Simulation (AMPS) last spring, Vice Admiral Art Cebrowski, Director J6 Joint Staff, emphasized the strides we are making in processing and storage. Specifically, he talked about speed and storage technology which doubles or triples every 18 months, laptops with the power of a CRAY and, most significantly pipes and software techniques which will allow data to be exchanged in the gigabyte and terrabyte range. Looking further into the future, we may see hardware without software and bandwidth may become virtually unlimited rather then the endpoint. With virtually unlimited processing and storage capabilities, we can have simultaneous running of combat models on the battlefield. Admiral Cebrowski further stated that many are afraid of being overwhelmed with data. However, he opined that would be wonderful. It then becomes a management problem...how we organize and make it available to the user at the right time at the right place.

To borrow another quote from Mr. Vince Roske, Joint Staff J8 made at the same AMPS symposium, "collaborative analysis is the name of the game". If the collaborative road is the road we are taking, it will be paved with the new information technologies such as the Defense Data Network, Defense Simulation Internet, videophones, JMCIS/GCCS, the Internet, and the list goes on. This collaborative technology is only in its infancy as we explode into a world where information transfer is characterized by fiber optics and massive satellite constellations which digitally link the advanced processing and storage capability we will have at our fingertips. It will be a world where battle labs do collaborative R&D analyses and test results on a virtual battlefield created at CINC analysis centers. It will be a world where DOD and industry collaborates to produce new designs and development using Simulation Based Design on High Bandwidth LANs. It will be a world where our fleets do collaborative planning to substantiate and prioritize their requirements as well as collaborative operational planning and rehearsal before and enroute to a crisis. The technology to allow collaborative analysis to be applied across the entire M&S spectrum before we build, before we buy and before, and even during, the fight is just emerging. What does all this suggest? Standardization. The point is, technology is driving us towards data standardization. The protocols and architecture which address standardization from the user and the generator perspective must be put in place now. This is the roadbed for building the collaborative highway. How will models and simulations service the "buckets of data" or repositories located at various stations along the highway? Will the DMSO sponsored Modeling and Simulation Resource Repositories fill that gap?

While DISA, OSD/DMSO, and the services are addressing data standardization, many issues remain to be solved. This article only briefly touches on a few of them. The problems associated with data are numerous and we, the analysts, the user community, have to deal with them. There are many organizations comprising many people spending millions of dollars working to solve these issues. What if we succeed in accomplishing data standardization? The associated changes, both in the culture and procedures of analysis, will be significant. Contractors might be provided models and simulations as Government Furnished Equipment. Certified data will be provided GFE. Resulting equipment models and data will be deliverables without any proprietary restrictions. Software and databases will be developed from a standard and become available as shareware/freeware on government/industry servers.

The result of all this new technology being applied to collaborative analysis is an analytical paradigm shift. It will change the way we analysts do business. The challenge of MORS is to lead the way in creating the analytical vision for the fu-

ture and then help survey the road ahead. We need full participation of the MORS experience to ensure that data architectures and standards are developed which follow that vision and meet our analytical needs. There will be bridges to be built which will cross rivers of cultural changes. The impact will be felt across both government and industry. To succeed we will need to dedicate the time, people, and resources to implement the process and follow it through over the long haul.

CAPT Lawrence L. (Lee) Dick is curretnly serving as Director, Warfare Analysis, Modeling & Simulation at Space and Naval Warfare Systems Command. A Surface Warfare Officer & Acquisition Professional, CAPT Dick received his Master of Science in Ops Research & Systems Analysis at Naval Postgraduate School in 1982.
He was selected as a MORS Director this past summer.

Appendix D

SIMDATAM Participants

Natalie S Addison
Military Operations Research Society
101 S Whiting Street
Suite 202
Alexandria VA 22304-3483
OFF TEL: (703)-751-7290
FAX: (703)-751-8171

Gregory P Andreozzi
USA Concepts Analysis Agency
8120 Woodmont Ave
Bethesda MD 20814
OFF TEL: (301)-295-1617 DSN: 295-1617
FAX: (301)-295-1834

John D Anzevino
Computer Sciences Corp
7115 South Boundary Blvd
MacDill AFB FL 33621-5101
OFF TEL: (813)-830-6430 DSN: 968-6430
FAX: (813)-830-4919

Rebecca Bace
DoD/R23
9800 Savage Road
Fort George G Meade MD 20755-6000
OFF TEL: (301)-688-0851

CDR Dennis R. Baer
Naval Center for Cost Analysis
NCA-54
1111 Jefferson Davis Hwy, Suite 400
Arlington VA 22202-4306
OFF TEL: (703)-604-0307 DSN: 664-0307
FAX: (703)-604-0315
E-mail: dbaer@dmso,dtic.dla.mil

MAJ Karen S Barland
AFSAA/SAG
1570 Air Force Pentagon
Washington DC 20330-1570
OFF TEL: (703)-697-5616 DSN: 227-5616
FAX: (703)-697-1226
E-mail: barland@afsaa.hq.af.mil

Michael F. Bauman
US Army TRADOC Analysis Command
ATTN: ATRC
Fort Leavenworth KS 66027-5200
OFF TEL: (913)-684-5132 DSN: 552-4689
FAX: (913)-684-6894
E-mail: baumanm@tracer.army.mil

David H Berg
HQ ACC/XP-SAS
204 Dodd Blvd
Langley AFB VA 23665-2778
OFF TEL: (804)-764-5460 DSN: 574-5460
FAX: (804)-764-7217

Walter Bowers
BATTELLE
1725 Jefferson Davis Highway
Suite 600
Arlington VA 22202-4172
OFF TEL: (703)-413-8866
FAX: (703)-413-8880
E-mail: bowers@battelle.org

Stephen T. Boyd
AFSAA/SAG
Nuclear Deterrence Division
1570 Air Force Pentagon
Washington DC 20330-1570
OFF TEL: (703)-697-5677 DSN: 227-5677
FAX: (703)-697-1226

DR Alfred G Brandstein
Marine Corps Combat Development Command
Studies and Analysis Division
3093 Upshur Ave
Quantico VA 22134-5130
OFF TEL: (703)-784-3235 DSN: 278-3235
FAX: (703)-784-3547
E-mail: algebra@usmc.mil

William C Burch
Integrated Systems Analysts, Inc.
Shirlington Gateway Suite 1000
2800 Shirlington Road
Arlington VA 22206
OFF TEL: (703)-578-2587

Linda Calvert
DMSO Support
1901 N. Beauregard Street
Alexandria VA 22311
OFF TEL: (703)-998-0660
FAX: (703)-998-0667

Carl E Carden
Integrated Systems Analysts
Suite 300
1843 Hotel Circle
San Diego CA 92108
OFF TEL: (619)-574-8100
FAX: (619)-574-8111
E-mail: ccarden@cod.nosc.mil

DR William A Carpenter
The MITRE Corporation
W548
7525 Colshire Drive
McLean VA 22102
OFF TEL: (703)-883-5777
FAX: (703)-883-3308
E-mail: wcarpent@mitre.org

Oscar A Chappel
National Simulation Center
Bldg 45, Attn: DIS
Fort Leavenworth KS 66027

DR Gregory H Chisholm
Argonne National Laboratory
9700 Cass Avenue, Bldg 900
Argonne IL 60439
OFF TEL: (708)-252-9295
FAX: (708)-252-5128

LTC Anthony H Colby
USMA
Systems Engineering
West Point NY 10996
OFF TEL: (914)-938-2700
FAX: (914)-938-5665

Cathy J Corley
Operational Analysis Center
255 SedgwickAnalysis Center
ATTN ATRC F MS CORLEY
Fort Leavenworth KS 66027-2345
OFF TEL: (913)-684-3030 DSN: 522-3030
FAX: (913)-684-8085
E-mail: corleyc@trac.army.mil

Donna Cornwell
MITRE
MS W548
7525 Colshire Drive
McLean VA 22102
OFF TEL: (703)-883-7011
FAX: (703)-883-3308

CAPT Lawrence L Dick
Space & Naval Warfare Systems Command
SPAWAR 31
Washington DC 20363-5100
OFF TEL: (703)-602-2791 DSN: 332-2791
FAX: (703)-602-5891
E-mail: dickl@smpt-gw.spawar.navy.mil

Robert C Figueroa
Cubic Applications, Inc., Suite 100
1901 N. Beauregard Street
Alexandria VA 22311
OFF TEL: (703)-578-5718
FAX: (783)-578-0060

Katherine Flood
UNISYS
Suite 300
1225 Jefferson Davis Hwy
Arlington VA 22202-4301
OFF TEL: (703)-604-6384
FAX: (703)-604-6400

Russell B Flowers
DOD
DIRNSA
9800 Savage Road
Fort George G Meade MD 20755
PHONE: (410)-859-4515

Charles E Gettig Jr
Gettig & Associates
Suite A
3500 Ada Dr
Mechanicsburg PA 17055
OFF TEL: (717)-732-9210
FAX: (717)-732-6002
E-mail: 73632,2613@compuserve.com

MAJ Phillip K Giles
US Army War College
Center for Strategic Leadership
Bldg 650
Carlisle PA 17013-5050
OFF TEL: (717)-245-3190 DSN: 242-3190
E-mail: gilesk@csl2emh1.army.mil

Howard P Haeker
TRADOC Analysis Command
Attn: ATRC-FSD
255 Sedgwick Ave
Fort Leavenworth KS 66027-2345
OFF TEL: (913)-684-3030 DSN: 552-3030
FAX: (913)-684-9151
E-mail: haekerh@trac.army.mil

Jeffrey L Hall
USA Concepts Analysis Agency
Attn: CSCA-RSD
8120 Woodmont Ave
Bethesda MD 20814-2797
OFF TEL: (301)-295-1660 DSN: 295-1660
FAX: (301)-295-1287

Wesley L Hamm
The MITRE Corporation
7525 Colshire Drive
McLean VA 22102
OFF TEL: (703)-883-6403
FAX: (703)-883-1379

MAJ Maureen R Harrington
HQ USAFA/DFCS
2354 Fairchild Drive
US Air Force Academy CO 80840-6252
OFF TEL: (719)-472-2136 DSN: 259-2136
FAX: (719)-472-3338
E-mail: mharring@cs.usafa.af.mil

DR Dean S Hartley III
Martin Marietta Energy Systems
Data Systems R&D Program
1099 Commerce Park
Oak Ridge TN 37830
OFF TEL: (615)-574-7670
FAX: (615)-574-0792
E-mail: dhx@ornl.gov

Robert G Hartling
Chief of Naval Operations (N812D)
2000 Navy Pentagon
Room 4A522
Washington DC 20350-2000
OFF TEL: (703)-695-3797 DSN: 225-3797
FAX: (703)-693-9760
E-mail: rhart@dmso.dtic.dla.mil

David F Hemingway
DESE
315 Wynn Drive, Suite 2
Huntsville AL 35805
OFF TEL: (205)-837-8004
FAX: (205)-722-7966

LtCol Danny L Hogg
The Joint Staff (J-8) ASD
Pentagon, Washington DC 20318-8000
OFF TEL: (703)-697-8899 DSN: 227-8899
FAX: (703)-693-4601
E-mail: dhogg@mhl.js.mil

Michael K Hopkins
Computer Sciences Corporation
USCENTCOM Combat Analysis Group
7115 South Boundary Blvd
McDill AFB FL 33621-5101
OFF TEL: (813)-828-6430 DSN: 968-6430
FAX: (813)-828-4919
E-mail: hopkins@cofs.centcom.mil

Myong Suk Kim
HQ USAF/XOMT
Suite 300
624 9th St., NW
Washington DC 20001-5303
OFF TEL: (202)-504-5340 DSN: 285-5340
FAX: (202)-504-5352
E-mail: mskim@xom-mail.hq.af.mil

Dennis A Konkel
US Army War College
Center for Strategic Wargaming
PO Box 534
Carlisle PA 17013
OFF TEL: (717)-245-4169 DSN: 242-4169

LtCol Kenneth C. Konwin
JAST/PIA
Suite 307
1745 Jefferson Davis Hwy
Arlington VA 22202
OFF TEL: (703)-602-7390 DSN: 332-7390
Ext: 664
FAX: (703)-602-0646
E-mail: konwink@ntrprs.jast.mil

Phillip A Kubler
US Army TRAC
ATTN: ATRC-F
Fort Leavenworth KS 66027-5200
OFF TEL: (913)-684-9176 DSN: 552-9176
FAX: (913)-684-9151
E-mail: kublerp@tracer.army.mil

Leslie E Lampella
HQ TRADOC
ODCS Analysis
ATTN: ATAN-ZA
Fort Monroe VA 23651-5143
OFF TEL: (804)-728-5953 DSN: 680-5813
FAX: (804)-727-4394
E-mail: lampell@monroe-emh1.army.mil

Al Lowrey
NRL
Code 6030
Washington DC 20375

Kevin MacDonald
Simulation, Training & Instrumentation
Attn: AMSTI-EE
12350 Research Pkwy
Orlando FL 32826
OFF TEL: (407)-389-2316
FAX: (407)-672-1396

Donald G Marks
DoD/R23
9800 Savage Road
Fort George G Meade MD 20755-6000
OFF TEL: (301)-688-0851

DR Susan Marquis
OSD (PA&E)
Crystal Gateway II, Suite 300
1225 Jefferson Davis Hwy
Arlington VA 22202
OFF TEL: (703)-604-6349 DSN: 224-6349
FAX: (703)-604-6400

DR W. T. Mayfield
Institute for Defense Analysis
1801 N. Beauregard Street
Alexandria VA 22311-1772
OFF TEL: (703)-845-6602
FAX: (703)-845-6848

Brian R McEnany
SAIC
1710 Goodridge Drive
T1-7-2
McLean VA 22102
OFF TEL: (703)-734-5849
FAX: (703)-821-1037
E-mail: mcenanyb@mcl.saic.com

Lana E McGlynn
US Army MSMO
Crystal Square II, #808
1725 Jefferson Davis Hwy
Arlington VA 22202
OFF TEL: (703)-607-3385 DSN: 327-3385
FAX: (703)-607-3381
E-mail: lana.e.mcglynn@pentagon-1dms18.army.mil

Janet Y Morrow
US Army National Ground Intelligence Ctr
Attn: IANG-RSG
220 7th Street, NE
Charlottesville VA 22901-5396
OFF TEL: (804)-980-7393 DSN: 934-7393
FAX: (804)-980-7699
E-mail: morrow@ca1.fstc.dodiis

Frank A Papineau
US GAO
OFF TEL: (703)-603-7721
FAX: (703)-603-7723

Mark H Ralston
US Army AMSAA
Attn: AMXSY-SL
Aberdeen Proving Ground MD 21005-5071
OFF TEL: (410)-278-6577 DSN: 298-6577
FAX: (410)-278-2788
E-mail: ralston@arl.mil

Jeffrey Allen Randorf
Space & Strategic Defense Command
PO Box 1500, Attn CSSD-SA-I
106 Wynn Drive
Huntsville AL 35807-3801
OFF TEL: (205)-726-3381
FAX: (205)-726-3909

Annette C Ratzenberger
National Simulation Center
410 Kearney Avenue
Fort Leavenworth KS 66027
OFF TEL: (913)-684-8304 DSN: 552-8304
E-mail: raty@tracer.army.mil

Todd H Repass
SPAWAR
Dept of the Navy M & S Tech Spt Group
2451 Crystal Drive, Suite 730
Arlington VA 22245-5200
OFF TEL: (703)-602-1788 DSN: 232-1788
FAX: (703)-602-5891
E-mail: repasst@smtp-gw.spawar.navy.mil

Michael G Rybacki
DMSMO
Crystal Square 2, Suite 808
1725 Jefferson Davis Hwy
Arlington VA 22202
OFF TEL: (717)-770-7131 DSN: 977-7131
FAX: (717)-770-6702
E-mail: rybacki@pentagon.hqdadss.army.mil

Phillip Taylor Salman
Booz Allen & Hamilton
Senior Consultant
1953 Gallows Road
Vienna VA 22182
OFF TEL: (703)-902-6926
FAX: (703)-902-7171

Stephen Scoville
The Joint Staff (J-8)
STP
Pentagon, Room 1D929
Washington DC 20318-8000
OFF TEL: (703)-697-0459
FAX: (703)-693-4601

Roy Scrudder
DMSO Support
CSC/C4I, Bldg 55350 Arizona Street
PO Box 719
Fort Huachuca AZ 85613-0719
OFF TEL: (602)-538-4812
FAX: (602)-538-4933

Darrel Sell
DoD/R23
9800 Savage Road
Fort George G Meade MD 20755-6000
OFF TEL: (301)-688-0851

Paul C Setcavage
Battelle
Pacific Northwest Laboratory
4001 North Fairfax Drive, Suite 600
Arlington VA 22203
OFF TEL: (703)-516-7440 DSN: 284-8747
FAX: (703)-243-5617
E-mail: pc_setcavage@pnl.gov

LtCol Robert S Sheldon
AFSAA/SAZ
The Pentagon, Room 1D386
Washington DC 20330-5420
OFF TEL: (703)-693-8423 DSN: 227-8423

Susan D Solick
TRAC-OAC
SDSD-V&V
Fort Leavenworth KS 66027-2345
OFF TEL: (913)-684-6868 DSN: 552-6868
FAX: (913)-684-4368
E-mail: solicks@tracer.army.mil

MAJ Walter L Swindell II
USA TRAC
Data Development Directorate
88 Hancock Ave
Fort Leavenworth KS 66027-1867
OFF TEL: (913)-684-3030 DSN: 552-3030
FAX: (913)-684-3866
E-mail: swindelw@tracer.army.mil

Clayton J Thomas FS
AFSAA/SAN
1570 Air Force Pentagon, Room 1E387
Washington DC 20330-1570
OFF TEL: (703)-697-4300 DSN: 227-4300
FAX: (703)-697-3441
E-mail: thomasc@afsaa.hq.af.mil

LtCol David S Thomen
Marine Corps Combat Development Command
Studies and Analysis Division
3093 Upshur Ave
Quantico VA 22134-5130
OFF TEL: (703)-784-3235 DSN: 278-3235
FAX: (703)-784-3547
E-mail: dthomen@dmso.dtic.dla.mil

Kenneth L Travis
TRW
OFF TEL: (505)-880-5135

Eugene P Visco FS
SAUS-OR
102 Pentagon, Room 1E643
Washington DC 20310-0102
OFF TEL: (703)-697-1175 DSN: 227-1175
FAX: (703)-697-7748
E-mail: visco03@ibm.dla.mil

DR Robert P Walker
Institute for Defense Analyses
1801 N. Beauregard Street
Alexandria VA 22311-1772
OFF TEL: (703)-845-2462
FAX: (703)-845-6722
E-mail: rwalker@ida.org

G. Karl Warmbrod
SPARTA Inc
Suite 900
7926 Jones Branch Drive
McLean VA 22102
OFF TEL: (703)-448-0210
FAX: (703)-734-3323
E-mail: karl_warmbrod@qmail.laguna.
sparta.com

MAJ Vicky C Watts
HQ DA Office of Deputy CS, Intel
Attn: DAMI-ST
1000 Pentagon Rm 2E453
Washington DC 20310-1000
OFF TEL: (703)-614-8121 DSN: 224-8121
FAX: (703)-697-8849

Alan E. Wetmore
US Army Research Laboratory
Battlefield Environment Directorate
AMSRL-BE-S
White Sands Missile Range NM 88002-5501
OFF TEL: (505)-678-5563

Howard G Whitley III
US Army Concepts Analysis Agency
Attn: CSCA-TCT
8120 Woodmont Ave
Bethesda MD 20814-2797
OFF TEL: (301)-295-1611 DSN: 295-1611
FAX: (301)-295-1287
E-mail: whitley@caa.army.mil

Richard I Wiles
Military Operations Research Society
101 S Whiting Street
Suite 202
Alexandria VA 22304
OFF TEL: (703)-751-7290
FAX: (703)-751-8171
E-mail: rwiles@dtic.dla.mil

COL Gerald J Wilkes
US Army War College
Center for Strategic Leadership
Bldg 650
Carlisle PA 17013-5050
OFF TEL: (717)-245-3171 DSN: 242-3171
FAX: (717)-245-3030

COL Stephen D Williams
US Army War College
Center for Strategic Leadership
Bldg 650
Carlisle PA 17013-5050
OFF TEL: (717)-245-3165 DSN: 242-3165
FAX: (717)-245-3279

DR Robert H Wright
Resource Consultants, Inc.
Suite 280
3051 Technology Pkwy
Orlando FL 32826
OFF TEL: (407)-282-1451
FAX: (407)-658-9541
E-mail: wright@msis.dmso.mil

Capt Roy D. Young
MCCDC
Studies & Analysis Division (C-45)
3093 Upshur Ave
Quantico VA 22134-5130
OFF TEL: (703)-784-3235 DSN: 278-3235
FAX: (703)-784-3547

LTC Mark A Youngren
Naval Postgraduate School
Code OR/Ym
Monterey CA 93943
OFF TEL: (408)-656-2281 DSN: 878-2281
FAX: (408)-656-2595
E-mail: myoungren@wposmtp.nps.navy.mil

MAJ Steve Zeswitz
MCCDC
Marine Corps Modeling & Simulation
2006 Hawkins Ave
Quantico VA 22134
OFF TEL: (703)-784-2588 DSN: 278-2588
FAX: (703)-492-9476